/*/

$3 7*

P. 141

# BREAKING DOWN BARRIERS IN COOPERATIVE FAULT MANAGEMENT: TEMPORAL AND FUNCTIONAL INFORMATION DISPLAYS

**Scott S. Potter and David D. Woods**

Cognitive Systems Engineering Laboratory
Department of Industrial and Systems Engineering
The Ohio State University
Columbus, OH 43210

# TABLE OF CONTENTS

iv

# LIST OF TABLES

# LIST OF FIGURES

# ACKNOWLEDGMENTS

# EXECUTIVE SUMMARY

This research has addressed the problem of how to aid human operators engaged in dynamic cooperative fault management. In this domain, a dynamic process is monitored for anomalous conditions by a joint cognitive system consisting of human operator(s) and an intelligent diagnostic system. More specifically, the focus of this work is on the coordination and integration of information from the monitored process and intelligent system to support operator visualization of critical events and anomalies in the process. To accomplish this, three phases of research were conducted. First, a series of case studies of intelligent fault management development projects was conducted to identify commonalities in the approaches used and to specify the human-computer interaction (HCI) demands imposed on the human operators. Based on these case studies, temporal, functional, and coordinative issues were isolated for further investigation. In the second phase, a series of descriptive models were developed to identify the inherent difficulties in the fault management task and the gaps between the information needed to cope with these demands and information currently (or typically) provided to an operator. The cognitive demands were used as a framework to uncover potential cooperation problems and the type of support required. Based on the results of the first two phases of work, the third phase involved the development of a specific design for one of the systems involved in the case studies, a thermal control system for NASA's proposed space station. This display design consists of coordinated functional and temporal representational views into the monitored process and the intelligent system. The goal of this design is to provide an enhanced temporal representation of the events and behavior of the system and the intelligent system's assessments, diagnoses, and recommended control actions in response to these events, to promote visualization of anomalous conditions within the process, and to coordinate and integrate information from the monitored process and intelligent system. One of the primary contributions of this work is the identification of the dependencies between efforts to develop an intelligent diagnostic system and efforts to build enhanced representational views for the human part of the cooperative ensemble.

# 1. INTRODUCTION AND OVERVIEW

## 1.1. Overview

At the highest level, the fundamental question addressed by this research is how to aid human operators engaged in dynamic fault management. In dynamic fault management there is some underlying dynamic process (an engineered or physiological process referred to as the monitored process – MP) whose state changes over time and whose behavior must be monitored and controlled. In these types of applications (dynamic, real-time systems), a vast array of sensor data is available to provide information on the state of the MP. Faults disturb the MP and diagnosis must be performed in parallel with responses to maintain process integrity and to correct the underlying problem. These situations frequently involve time pressure, multiple interacting goals, high consequences of failure, and multiple interleaved tasks (Woods, 1988a).

Some of the difficulties of this task include:

- system complexities (e.g., structural, functional, and temporal) result in a difficult diagnosis task,
- an abundance of low-level sensor data result in a data overload (a large amount of data to sift through and comprehend),
- the need to shift attention across the incoming data as events and changes occur within the MP, and
- the need to anticipate future changes and behavior in the MP.

At this level, some of the goals of aiding fault management are to:

- provide a clear representation of MP status and behavior,
- provide support for the detection of anomalous MP behavior and the mapping of symptoms into causes of anomalous behavior,
- integrate the abundance of data from sensors into information relevant to process goals and tasks, and
- help focus operators' attention on critical information within the MP.

One trend in dynamic fault management is the addition of artificial intelligence based systems to assist the human operator. This creates a joint human-machine cognitive system that should function cooperatively to handle the demands of dynamic fault management. Depending on the nature of the interaction between the human and the intelligent system (IS), the fault management task can become more or less demanding. On one hand, the additional source of information could actually add to problems such as data overload and directed attention. In addition, depending on the types of representational windows provided for the human operator, barriers can be created that make it difficult for the operator to see the IS's line of reasoning, to see what the IS thinks is going on in the

1

MP, or even to see the flow of events in the MP itself. On the other hand, if successfully coordinated, these multiple sources of information could provide complementary views into the behavior of the MP and assist the operator in assessing MP status and responding to anomalies.

Thus, the fundamental question addressed by this research is how to integrate human and machine problem solvers into an effective cooperative system. More specifically, the focus is on the coordination and integration of information from the MP and IS to support operator visualization of critical events and anomalies in the MP and the IS's assessment, diagnoses, and recommended control actions in response to these events. In order to study this problem, three phases of research have been conducted. They are outlined in the following sections.

## 1.2. Phase I: Critique of IS as cooperative agent

The first phase of research consisted of a series of six case studies of intelligent fault management system development projects in which human-computer interaction (HCI) capabilities, cooperative problem solving issues, and the design process used were examined (Malin, Schreckenghost, Woods, Potter, Johannesen, Holloway, and Forbus, 1991a,b; Woods, Potter, Johannesen, and Holloway, 1991a,b). The types of systems studied included efforts at developing and implementing diagnostic reasoning systems to assist operators in controlling a semi-autonomous process. The core of these case studies consisted of aerospace systems being designed for NASA's Space Station (consisting of thermal, electrical, and environmental control systems; Potter and Woods, 1992a,b,c – see Appendices A, B, and C).

In general, these case studies revealed designers using color graphic, multiple window interface capabilities in an attempt to expand the communication bandwidth between the human and intelligent system. Some of the approaches found in the case studies include:

- physical topology schematic displays annotated with digital sensor values as the primary medium for presenting information on the state of the MP,

- chronologically ordered message lists as primary source for displaying IS diagnoses, recommendations, etc. as well as for logging MP events (e.g., mode and configuration changes, sensor limit violations),

- user definable workspace design (i.e., permit the operators to position windows anywhere, call up any number of windows), and

- active (mousable) regions within schematic displays to access additional information about a specific sensor, component, or process.

However, previous research has shown that building such a decision support system does not guarantee that the practitioner will find the system useful (Woods, Roth, and Bennett, 1990). Results from this phase of research lend support to this claim through the identification of a variety of common barriers that can impede human-intelligent system cooperation. Some of the problems include:

- lack of tools to help the operators visualize the state of the system (i.e., highlight events) and the functional impact of faults that have occurred (physical schematics emphasize physical, rather than functional relationships),

- failing to capture any of the temporal information within the fault management task such as event onset and offset and temporal relationships and dependencies between events (chronologically ordered message lists compress the informational and temporal aspects of events),

- failing to embed IS output into the context of changes in the MP (multiple window workspace design encourages dissociation of related information), and

- lack of depicting relationships between changes in the MP and resulting IS diagnoses (message lists combine asynchronous, multidimensional information into a unitary format).

## 1.3. Phase II: Cognitive task analysis and model development

Based on the results from the case studies, three dimensions have been abstracted for further investigation: *functional, temporal,* and *coordinative.* They are outlined in the following paragraphs.

**Functional** refers to how a MP works to accomplish relevant goals. This type of information is concerned with goal-relevant relationships between data which provide insights into system status and function (e.g., is $x$ within normal range? how much capacity in $y$ is left?) rather than simply current measured values ($x = 80$ psi; $y = 30$ amps). Additionally, functional relationships between components (how change in one component functionally impacts others) can be contrasted with physical relationships (physical interconnections between components) to understand system dynamics. There has been considerable work on the contributions of functional modeling as an approach to develop user interfaces to complex systems (Rasmussen, 1986; Vicente and Rasmussen, 1990; Woods and Hollnagel, 1987; Lind, 1991). It is important to note that this is based on the same principles that form the basis for functional modeling as an approach to building intelligent diagnostic systems (K. Abbott, 1990).

**Temporal** refers to several relationships based on time. First is the fact that dynamic system parameters change continuously over time; second is the event-based, qualitative temporal relationships between events (i.e., process A ended before process B started). Both types of temporal information can play an important role in developing intelligent reasoning systems (Allen, 1984). In addition, a group of researchers recently have begun investigating the importance of time in investigating human interaction with complex systems (Decortis, De Keyser, Cacciabue, and Volta, 1990).

**Coordinative** refers to the coordination of information from the MP and IS to *jointly* convey to the human operator what is going on within the MP. Results from Phase I (and from previous research – Shafto and Remington, 1990) revealed that information from the MP and IS typically are dissociated rather than coordinated and integrated. This coordination can (and will) be discussed in two directions and at several levels. First, within a representation of the MP (physical or functional), the

IS's dynamic, real-time computations can provide informative context in which to interpret MP behavior. For example, Chapter 5 will discuss the use of expected current and predicted future values generated by the IS to provide a reference against which to compare current TCS conditions. Second, within the representation of the IS's activity, establishing a linkage from an IS's diagnosis back to the causal events in the MP can be an important aspect of explanation. Chapter 4 will discuss the use of graphical approaches to building this causal relationship. Third, it is important that information across multiple views (or perspectives) be coordinated and work together to provide the human operator with insights into MP status, as opposed to forcing serial access to data through multiple views. Chapter 6 will discuss the joint use of the functional view of the MP and the temporal view of the IS as an overview display. This need for coordination between information sources (MP and IS) builds on the idea of building a common, or shared frame of reference (Woods and Roth, 1988) to improve the communication between the human operator and IS in jointly monitoring and controlling the MP.

Within this framework, an investigation of information requirements of the human operator in dynamic fault management and information availability from the MP and IS was performed. The primary goal of this phase is to identify the inherent difficulties in the fault management task and the gaps between the information needed to cope with these demands and information currently (or typically) provided to the operator. The cognitive demands were used as a framework to uncover potential cooperation problems and the type of support required. The basic finding was that the typical approaches (of physical topology schematic displays and chronologically-ordered message lists) vastly under-specify the informational demands of the diagnostic task and requirements of the operator.

One of the guiding mechanisms in this phase of research is a series of descriptive models of the interaction between the three agents (human, MP, and IS) at several levels of specificity. First, a generic, context-free model of dynamic fault management is used to lay the foundation for the types of cognitive activities required. Second, a mid-level, context-relevant model was developed from specific examples abstracted from the case studies. This focuses on the temporal and coordinative dimensions. Third, a system specific functional model was developed based on an analysis of system objectives for a particular MP (introduced in the next section). These latter two types of models also provide a framework for determining what information needs to be included in the design of alternative representations. This is the focus of Phase III.

## 1.4. Context: Thermal control system

The application domain for this effort is NASA Space Station Freedom's (SSF) Thermal Control System (TCS). The TCS is being designed to maintain thermal conditions within SSF crew and experimental quarters and to reject excessive heat into space. One of the primary system requirements is the ability to adjust internal conditions and efficiency of heat rejection to balance widely varying heat loads (as activities and experiments change). This is a very elegant and complex system in which virtually all of the control is passive, allowing for great range of adaptation to

changes in thermal conditions without any intervention. At the same time, though, this elegance also complicates diagnosis, as faults can be "masked" by make-up systems and redundancies within the system.

The TCS accomplishes its goal by the use of three main subsystems – a set of evaporators, a transport loop (for pumping and inventory control), and a set of space radiators (condensers). The evaporators acquire heat, the condensers reject this heat to space, and the transport loop maintains inventory and temperature/pressure equilibrium within the system and provides pressure differentials ($\Delta p$) to "pump" inventory throughout the system.

TCS was selected for this investigation because of several characteristics:

- there are close functional interconnections between system components. As a result, a fault produces symptoms and disturbances in multiple areas over time,
- the system has a significant temporal dimension (time for liquid and vapor to traverse through the system) which creates additional complexity in diagnosis,
- considerable attention is being directed toward the development of an intelligent diagnostic system, and
- the development of a thermal test-bed, a ground-based system to test the above mentioned IS (as well as hardware changes to the TCS).

## 1.5. Phase III: Representation design

Based on the results from the critique of human-IS cooperation in fault management, the development of generic HCI concepts and a specific design for the TCS is the focus of the third phase of research. In particular, the goal of this design effort is threefold:

- to provide an enhanced temporal representation of MP events and IS activity,
- to promote visualization of MP events (e.g., changes in the pattern of disturbances over time), and
- to coordinate and integrate information from the IS and MP (which, from phase I results, is typically dissociated) in order to indicate relationships between the two sources of information and use one as a reference for interpreting the other.

Specifically, this phase is concentrated on illustrating the structure and behavior of this type of display system, focusing on its ability to support cooperative fault management activities.

This phase focuses on two approaches to achieve this goal. The first is a new type of representation of the intelligent system's communication to the human operator. As identified in Phase I, information from the intelligent system is typically presented to the human operator in the form of chronologically ordered message lists. However, examples from Phase II demonstrate that this representation does not assist many of the operator's diagnostic activities. Specifically, this form does not capture any of the temporal or relational information that is required or the event-driven nature of the task (Potter and Woods, 1991). Therefore, based on the investigation of temporal characteristics of fault management (Decortis, et al., 1991) and on a descriptive model of information

requirements, a display concept to supplant message lists – a *temporal information display* – has been developed.

The second approach is the coordination and integration of information from the IS into a view of the MP as a means to enhance cooperation between the IS and the human operator (Potter, Woods, Hill, Boyer, and Morris, 1992). Typically the representational window on the MP in fault management systems consists of raw telemetry data organized by the physical anatomy of the MP. While the IS may derive higher level information about the state of the MP by collecting and integrating raw data values, little of this information is integrated into an operator's display of the state of the MP. For example, the IS may use models of MP structure and function to dynamically compute expected behavior over a wide range of conditions; but often the IS's expectations are not captured and made available to the human. Therefore, this phase of the research also describes the development of an integrated *function-based display* as another means to enhance cooperation between an IS and its human partner(s).

This basic concepts behind the temporal information display design are to provide the following:
- linkage between MP events and resulting IS activity,
- temporal relationships between events,
- micro and macro views to provide overview as well as detailed information, and
- navigation features (e.g., search and zoom) to maneuver through the messages.

For the function-based display, the key features of this display are:
- enhanced visualization of events and anomalies,
- depiction of higher-order functional properties and relationships, and
- use of IS information as context in which to interpret behavior of the MP.

Additionally, attention has been given to the coordination of these two representational views to provide one integrated view of the systems' events and activities. The key features of this aspect of the displays are:
- overlapping windows to create different views to emphasize different aspects of the system and
- coordination of the two displays as information management tools.

## 1.6. Contributions and future directions

Previous IS development work on the TCS has provided some insights into the problem addressed by this research (Shafto and Remington, 1990). They found that operators did not make extensive use of an independent representation of IS results; rather, they validated diagnoses by referring to a representation of the MP itself. Since the representation of the MP consisted of raw telemetry data, this type of interface encouraged a minimally-cooperative architecture of independent problem solving and cross checking which has been shown to be a very weak style of coordination in distributed cognitive systems (Roth, Bennett, and Woods, 1987).

It is expected that this research will provide a foundation for moving from weaknesses in typical approaches to human-intelligent system-interaction (H-IS-I) in fault management to approaches that enhance the operator's visualization of events in the MP and the diagnostic activity of the IS in response to these events. At a global level, this should improve the communication between the three agents and thus increase total system performance. At another level, it is expected that the approach employed for integrating IS output in a form that represents the temporal and relational nature of the domain would be applicable to a wide variety of fault management applications. Thus, the design concepts for temporal information displays should be an integral part of any IS display design for cooperative fault management. Also, this work extends the utility of the functional modeling work to another domain with different attributes (cyclical, mass balance vs. directional flow in Vicente and Rasmussen, 1990). Specifically, this approach was very useful in identifying information deficits in building the representation of the MP (that, in some cases, were filled by the IS).

Additionally, as this work has been exploratory and design-focused in nature, there are several directions for future work which should be explored. First, this effort revealed the need for further exploration of the use of temporal information in fault management. The development of the temporal information display is one representation of time. Interviews with TCS operators revealed a heavy reliance on temporal information that needs to be integrated into an overview display. Second, while this work has attempted to address the need for coordination of information across multiple information sources and perspectives into the process, this problem needs to be continued in the development of complete systems (i.e., this project did not address the coordination between the overview display and other, more detailed displays). Third, it was found that, in accord with previous research (Woods and Roth, 1988) tools (representations) shape their use by practitioners. Thus, it is important to support (and build on) operators' current models and understanding of the process through the user interface while providing additional information and tools to enhance the operators' awareness of system properties. These issues will be discussed in Chapter 7.

## 1.7. Organization for subsequent chapters of this report

**Chapter 2 – Cooperative fault management:** Section 1 discusses fault management, including the nature of the cognitive demands on the human operator. Additionally, this chapter includes a description of an information processing model for describing human performance in fault management. Section 2 discusses relevant knowledge and research on human-intelligent system interaction that may apply to the problem area of this work.

**Chapter 3 – The research application: Thermal control system:** This chapter provides a detailed description of the application under investigation (TCS). Based on this description the system dynamics, elegance, and complexity will be apparent. Additionally, several scenario-based descriptions are included to depict the behavior of the system.

**Chapter 4 – Tracking intelligent system activity: Development of temporal information displays:** This chapter describes the temporal aspects of cooperative fault management and their impact on the information presented to the human operator. Second, it includes characteristics,

weaknesses, and potential alternatives to traditional approaches. Based on this information, this chapter also presents design concepts for the development of information displays for the IS to communicate to the human operator.

**Chapter 5 – Visualization of monitored process behavior: Development of function-based displays:** This chapter describes the functional/structural aspects of fault management and their impact on information requirements for a human operator. It also includes a critique of typical physical schematic displays. Third, it presents the development of a function-based display design for the TCS.

**Chapter 6 – Representation design:** The information in the preceding two chapters provides a basis for the particular implementation (and test vehicle) for this research. This chapter provides a description of the relevant attributes of this design and a dynamic "walk-through" of its behavior.

**Chapter 7 – Conclusions and recommendations:** This chapter discusses the contributions of this research and potential future directions.

# 2. COOPERATIVE FAULT MANAGEMENT

## 2.1. The research domain: Fault management

### 2.1.1. Overview

As mentioned in the previous chapter, the target application for this work is a human operator and an intelligent system (IS) engaged in the joint monitoring and control of an engineered system (denoted MP for monitored process), whose state changes over time (as indicated in Figure 1). In fault management the MP must be monitored for the occurrence of anomalous situations and behavior which may arise within the setting of a continually changing state. Once a fault has been detected, attention must be given to determining the causes of anomalies, and repairing anomalies for the MP while maintaining safety and the ability to perform planned operations. There are three main goals in fault management:

- monitoring and fault detection,
- safing, mission impact assessment, and reconfiguration, and
- fault isolation, testing, and recovery.

The predominant behavior during normal situations, though, is detecting significant changes in dynamic data indicating off-nominal behavior.

However, these activities must occur simultaneously, as the MP typically cannot be removed from service for diagnosis. This means that the fault manager needs to try to continue to meet the goals of the monitored process (Woods, 1988a). The relative importance of different process goals may change as the incident evolves and some goals may need to be abandoned if they compete with more critical goals (mission control activities following the oxygen tank explosion during Apollo 13 are a good example of this). A summary of characteristics of fault management is provided in Table 1.

### 2.1.2. Cognitive demands of fault management

#### 2.1.2.1. System demands

There are several aspects of fault management that make the task difficult to perform. First, the MP is typically a complex system. One can think of complexity along several dimensions:

- structural complexity (large number of components with multiple connections),
- functional complexity (significant, diverse capability), and
- temporal complexity (large difference in the response times between the MP and the human operator).

Second, the quantity and quality of data is demanding. There is typically a large amount of data about the state of the MP, resulting in high data rate. The vast amount of data must be synthesized and integrated in order to be informative and not overload the human operator.

In addition to quantity, the quality of data can complicate the fault management task. There can be uncertainty in the sensed data (through sensor and transmission failures) and the models of expected behavior (through a mismatch of assumptions and environmental characteristics).

## 2.1.2.2. Performance demands

In fault management, the operator may need to satisfy multiple competitive goals in the face of incomplete and often contradictory information. There is high pressure to perform efficiently (the need to get through a certain number of operations each day, or to land a certain number of aircraft per hour), and omnipresent in the background is the fact that the mission may fail or the plane may crash. The expert in these worlds is often confronted with resource saturation, especially at high criticality time periods. The strategies that experts use to cope with these demands is particularly relevant to those who would design information systems to support their activities.
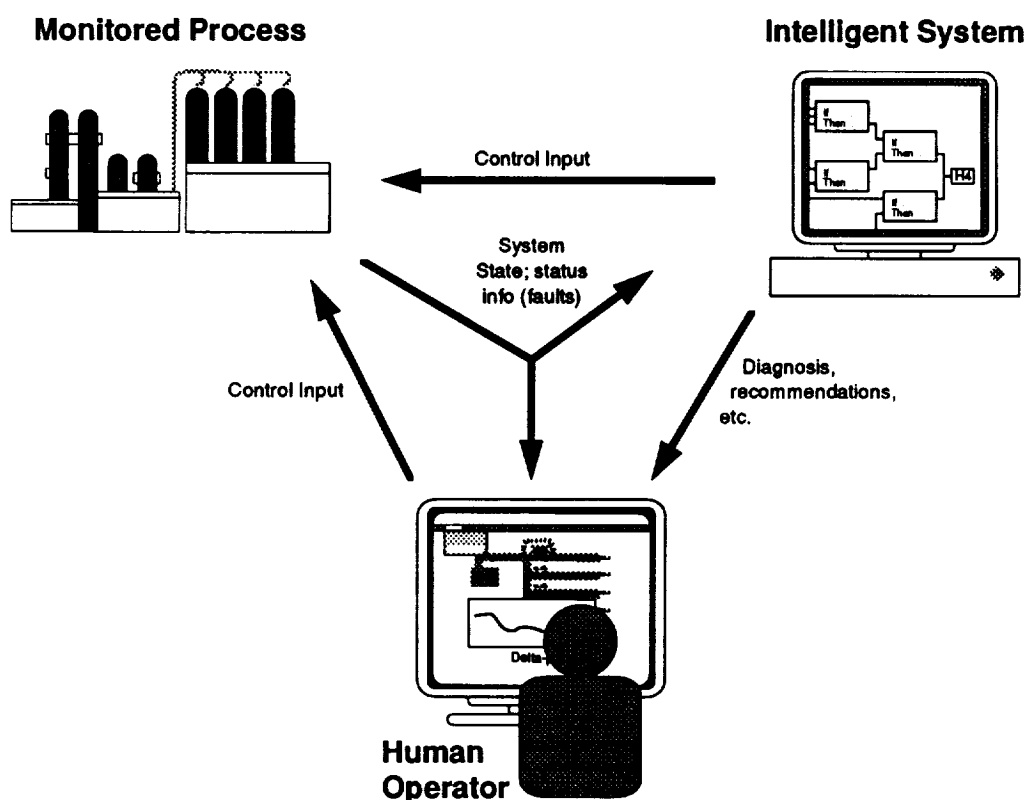


Figure 1. Depiction of information flow in fault management.

Expert performance is more than simply following a plan or collection of guidelines. Rather the expert is one who can adapt plans, bring new plans into being and cancel others as new events warrant, and maintain several threads of action in different stages of completion. The critical contribution of people to the person-machine ensemble is adaptability in the face of the variability and surprise of real, complex situations (Rasmussen, 1986; Woods, 1988a). This adaptability means that experts can handle special cases and exceptions as well as routine cases; to use efficient reasoning shortcuts but then to switch to more thorough reasoning strategies when cues indicate that the present case is atypical. Based on this, Hollnagel (1992) claims that the main feature of an intelligent system is that it should be able to modify its own behavior or be adaptive.

The human operator must track evolving situations loaded with unanticipated and potentially threatening events. As a result, operators must build and maintain a coherent situation assessment in

Table 1. Characteristics of aerospace fault management (adapted from Malin, et al., 1991; Woods, 1988).

**Complexity:**

- Resident in hostile, constrained environment (e.g., microgravity).
- Remoteness of control.
- Complexity of engineered systems (structural and functional).
- Continuous, long duration support periods for operators.
- Multiple tasks performed in parallel by multiple operators.

**Dynamism:**

- Real-time constraints and performance requirements.
- High data rates due to physical dynamics.
- Large amounts of information due to complexity of systems and operations.
- Dynamics often outside range of human perception.
- Frequent interruptions during critical operations.

**Uncertainty:**

- Deficiencies in information (data and models of behavior).
- Unavailable information (inadequate sensors, limited bandwidth transmissions).
- Limited resources in task environment (both human and expendable).
- Unanticipated situations.
- Decisions under conditions of uncertainty.

**Risk:**

- Decisions under conditions of high risk due to the cost of errors.
- Criticality of making correct response.

a changing environment where multiple factors are at work including one or more faults, operator interventions and automatic system responses. How do people evaluate large amounts of potentially relevant and changing data in order to size up a situation in the face of time pressure? Researchers who examine expertise in situ have noted that practitioners themselves coin various phrases that describe the ability to maintain this coherent view of changing situation: in commercial aviation it is referred to as being "ahead of the plane", in carrier flight operations the expression "having the bubble" is used (Roberts and Rousseau, 1989), in military operations von Clausewitz (1968) called it "coup d'oeil" – the ability to discern where and when a decisive action can be taken.

Attentional control in the face of multiple interleaved activities and the possibility of asynchronous and unplanned events is a fundamental part of fault management. Experts need to be able to manage several threads of activity in parallel, devoting enough attentional resource at the appropriate time in order to keep each on track. Also at issue here is interrupt handling – as data changes and new events are noted, how do they or should they modify the current task or cognitive resource priorities. Understanding action in the face of diverse, changing and highly uncertain situations depends critically on understanding attentional processes and the dynamic prioritization of tasks. A critical criterion for the design of the fault management systems is how they support operator attention focusing, attention switching and dynamic prioritization.

### 2.1.2.3. The cascade of disturbances

In dynamic, uncertain, and dangerous domains, fault diagnosis occurs as part of a larger context where the expert practitioner must maintain system integrity by coping with the consequences of faults (i.e., disturbances) through safing responses in parallel with untangling the causal chain that underlies these disturbances in order to take corrective responses. The interaction between these two lines of reasoning and activity defines a major cognitive activity of human experts in dynamic problem solving situations, what Woods (1988a) has called the *disturbance management cognitive task.*

Fault management in dynamic applications has a different character than the stereotype about diagnostic situations which is based on the exemplar of troubleshooting a broken device which has been removed from service. In dynamic process applications, fault management incidents extend, develop and change over time. A fault disturbs the monitored process and triggers influences that produce a time dependent set of disturbances (i.e., abnormal conditions where actual process state deviates from the desired function for the relevant operating context). This cascade of disturbances unfolds over time due to the development of the fault itself (a leak growing into a break) and due to functional and physical interconnections within the monitored process (Woods, 1988a; K. Abbott, 1988, 1990).

Figure 2 provides an aviation illustration of the cascade of disturbances that can follow from a fault (K. Abbott, 1990). The initiating fault is a failure in the fan subsystem of an aircraft engine. This fault directly produces an anomaly in one engine parameter, but the fault also disturbs compressor function which is reflected symptomatically in an anomaly in another engine parameter. The effect

of the fault continues to propagate from the compressor to the combustor producing anomalies in two more engine parameters. Diagnosis involves understanding the temporal dynamics of the cascade of disturbances. For example in this case, the temporal progression is an important clue to understand that the fault is in the fan subsystem and not in the compressor or the combustor. Note that, because of disturbance propagation, the same or a similar set of anomalies may eventually result from a fault in a different subsystem. A critical discriminating difference is the propagation path as the cascade of disturbances develops over time.

### 2.1.2.4. The alarm handling problem

As mentioned earlier, a critical characteristic of a fault management system from a cognitive point of view, is how it helps segregate the relevant variations from the irrelevant ones. And the critical constraint on carrying out this cognitive function is the context sensitivity problem – which variations are important depends on the state of the process itself and on the state of the problem solving process. We can term this the alarm handling function of a fault management system.

There are classic paths that have been used to cope with the alarm handling demands of fault management. One is to develop a fixed, static priority assignment to individual alarm signals. Usually, two or three classes of priority are defined and then individual alarm signals are assigned to one these categories. Presumably, there are only a few high priority alarms that occur in the same
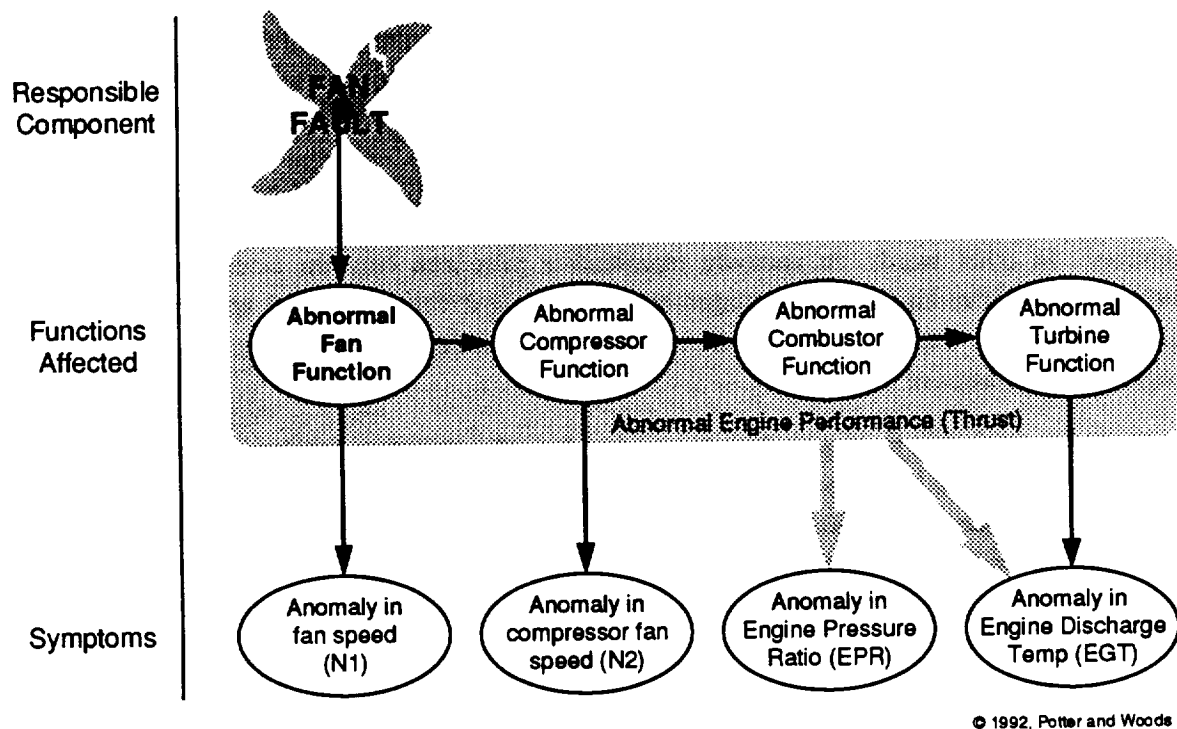


Figure 2. Cascade of disturbances for an aircraft engine fault (adapted from K. Abbott, 1990).

time period and alarms in the lower priority classes do not need to be processed in order to evaluate the significance of the high priority ones. In other words, the static priority technique tries to cope with alarm handling demands through a scale reduction process.

Another classic technique is to develop automated fault diagnosis. The need to handle alarm information is avoided by simply developing a machine to do the diagnosis via heuristic or algorithmic computer processing. The automated diagnostic system processes the alarm information and determines what fault or perhaps what faults are present in the monitored process. When the system has determined a fault, the human operator is notified of the result. Now, the fault determination is often softened (in part because of reliability concerns) and output with an attached "degree of belief" marker, as a ranked list of hypotheses, or as a recommendation. Nevertheless, all of these approaches attempt to cope with the alarm handling demands of fault management through a finesse of allocating the task to a machine rather than supporting the human operator.

## 2.1.2.5. Information processing in fault management

Information processing in fault management is anomaly driven (as illustrated in Figure 3). There are a large number of data channels and the indications on these channels may be changing (the left side of Figure 3). The first task of a fault management system (either human alone, machine alone or the ensemble) is to recognize, out of all the signal states and changes, which represent anomalies – significant findings about the current and future state of the monitored process. Obviously, this can be relatively easy when all data channels are quiescent except for one. But faults in the monitored process produce multiple effects that change over time creating the potential for an avalanche of changing indications. This is an example of a potential data overload situation where the critical cognitive activity is filtering the relevant indications from the irrelevant variations in the disturbed process (Woods, 1992).

In everyday usage, an anomaly is some kind of deviation from the common order or an exceptional condition. In other words, an anomaly represents a mismatch between actual state and some standard. To characterize a fault management system cognitively, one must specify the different kinds of anomalies that the system can recognize and information processing that is needed to recognize these classes of events.

One kind of anomaly has to do with departures from desired system function for a given context (i.e., the monitored process is not performing the way it was designed to perform). It could be that pressure is supposed to be within a certain range but that it is currently too low. This class of anomalies can be described as "abnormalities," that is, observed monitored process behavior is abnormal with respect to the desired system function for a particular context (e.g., shutdown versus full power operations).

Another kind of anomaly has to do with process behavior that deviates from the operator's model of the situation. In this case process behavior deviates from someone (the operator's) or something's (the intelligent system's) expectations about how the process will behave. The agent's expectations

are derived from some model of the state of the monitored process. Because the present focus is on dynamic processes, this model refers to the influences acting on the process – influences resulting from manual actions, influences resulting from automatic system activities, or influences resulting from the effects of faults. Anomalous process behavior that falls into this class can be called "unexpected," that is, observed monitored process behavior is unexpected with respect to model derived expectations for the particular context.

For example, if a power generation system trips and there is some kind of cooling reservoir in the system, then level in that cooling reservoir is going to drop. It always drops when the power generation system is shut off. Thus, a low level alarm indicates an abnormality with respect to the desired system function; however, the alarm is expected given the circumstances. The operator knows "why" the alarm indication is present (it is an expected consequence of the influence of the rapid shutdown) and therefore this alarm does not interrupt or change his or her information processing activities (e.g., the operator will not try to "diagnose" the fault). What would be unexpected would be the absence of this alarm or if the low level condition persisted longer than is expected given the influence of the trip event. Note that there can be other kinds of anomalies as well, for example, departures from plans.



© 1991, Woods, Potter, Johannesen, and Holloway
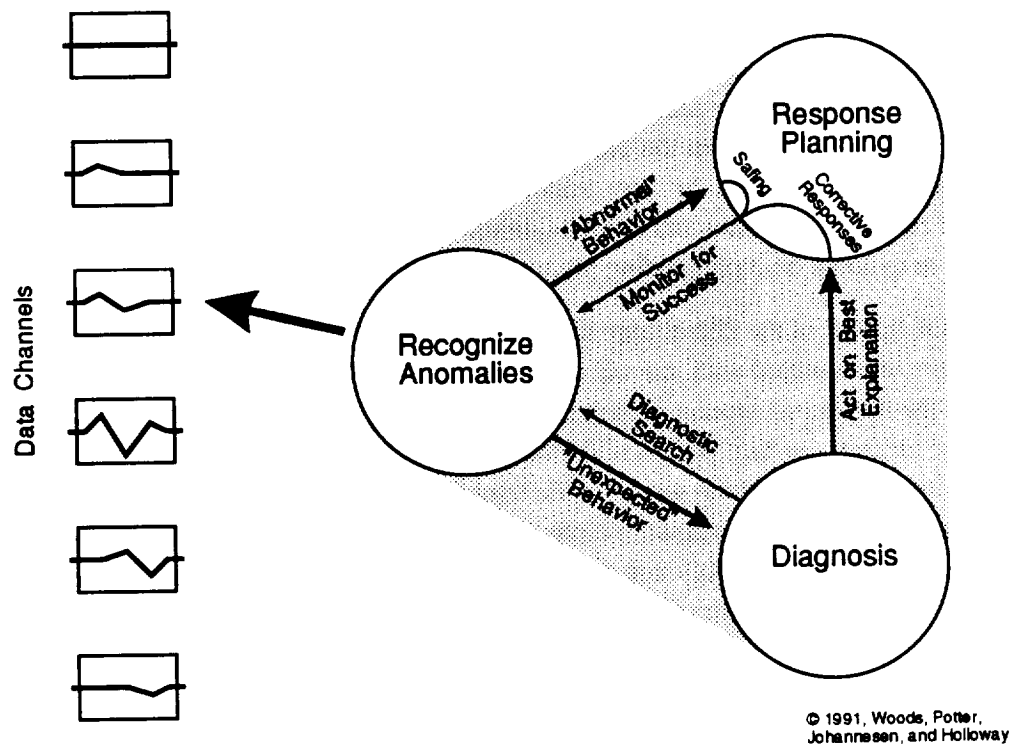
Figure 3. Model of anomaly-driven information processing in dynamic fault management.

As indicated in Figure 3, recognition of "abnormal" process behavior should lead to information processing about how to cope with the indicated disturbance, for example, safing responses. This, in turn, leads to monitoring lines of reasoning – checking to see if coping responses have occurred as expected and whether they are having the desired effect. Thus, in the above example, the low level alarm should trigger a line of reasoning to evaluate what coping responses should be initiated to deal with the abnormality, for example, an automatic makeup system should start up to resupply the reservoir and a line of reasoning to monitor that the automatic system came on properly and is restoring level to the desired range. Recognition of "unexpected" process behavior should lead to diagnostic information processing – a line of reasoning to generate possible explanations or "diagnoses" for the observed anomaly and knowledge-driven search to evaluate the adequacy of those possible explanations. When a diagnosis is reached (a best explanation), it can trigger a line of reasoning to identify or develop corrective responses.

This model of the cognitive activities in fault management has several implications for the design of intelligent systems to support fault management. One is that the fault management support system should help the operator see anomalies in the monitored process. Since anomalies are defined as mismatches, the fault management support system should help the operator see what specific mismatch is present. Since there are different kinds of standards for process behavior, e.g., target values, limit values, automatic system response thresholds, intelligent system "expectations" (in the case of model based AI systems), indications of an anomaly should include the standard violated.

Cognitive activities in fault management involve tracking the set of anomalies present in the process and their temporal inter-relationships. Fault management support systems can help operators see the dynamics of anomalies and the underlying disturbances in process functions, especially to see how disturbances grow and subside in the face of safing/corrective responses (Woods, Elm, and Easter, 1986). This information may be very important in the diagnostic process and in the strategic allocation of cognitive resources either to diagnostic search to identify the source of the cascade of disturbances or to focus on coping/safing actions to protect important goals.

A fundamental feature of the disturbance management cognitive task is that diagnostic activities and information are intermingled with manual and automatic responses to cope with the consequences of faults. How the monitored process responds to these coping/safing actions provides information for the diagnostic process. In fact, people will often take actions whose primary purpose is to check out or confirm a hypothesis about the source of the trouble – diagnostic interventions. It is important for an "ideal" fault management support system to assist the human operator untangle the interaction between the influences of fault(s) and the influences of coping/safing actions taken by automatic systems or by some of the people involved.

## 2.2. Human-Intelligent system cooperation in fault management

### 2.2.1. Introduction

The question to be addressed is how are the fault management operations described in the previous section affected by the introduction of an intelligent system? First, the introduction of an IS distributes activities between agents. This brings in the need to coordinate the activities of the agents. Also, the IS represents a new source of information for the human operator. Therefore, the use of an IS increases the need for innovative information management approaches to handle the already large amounts of information used for fault management. Typically, ISs are designed for one-way communication. However, often the information provided by an IS is not particularly informative, consisting of statements or recommendations with no context for interpretation or clarification of the reasoning behind the conclusions. ISs are subject to errors also. They can be brittle, failing catastrophically in situations that exceed the bounds of their encoded knowledge. Thus, an IS must be monitored by the human operator (Malin, et al., 1991a).

One can think about the problem of human interaction with intelligent systems at two levels. At a concrete level, human interaction can be thought of in terms of the computer interface between the human operator and the intelligent system – the graphic displays available, the window structure, the dialog mechanisms that support moving around in the interface or that support communication with the intelligent system. But at a deeper level, design of the interaction between practitioner and the intelligent system requires an explicit definition of the roles of each, as well as consideration of an appropriate cooperative problem solving approach for a particular application. The following sections explore some of the relevant issues in cooperative problem solving (cf., also, Woods, 1986b; Woods, Roth and Bennett, 1990; Robertson, Zachary and Black, 1990; or the bibliography in Woods, Johannesen and Potter, 1990).

### 2.2.2. Related research on cooperative problem solving

#### 2.2.2.1. Human-human advisory interactions

Support for concepts relevant to human-intelligent system interaction has been found in empirical studies of human-human interaction. The basis for studying humans interacting in a cooperative manner is that, if successful, it should provide support for key aspects of H-IS-I.

Coombs and Alty (Alty and Coombs, 1980; Coombs and Alty, 1980, 1984) studied computer users who solicited the advice of experts for diagnosis and correction of software failure. They assert that human experts are often asked to provide conceptual guidance to other experts in adjacent fields to enable them to solve problems for themselves. The critical difference, they argue, between the role of an expert as a problem solver and as an advisor is that:

> "while the former focuses upon the process of obtaining a concrete, communicable solution to a problem, the latter is primarily concerned with the enrichment of the user's understanding of a problem area and the development of his skills at handling that area. As an advisor, the expert is expected to support a colleague's personal problem solving,

particularly at the junction between their two areas of expertise, and to help him decide what questions should be asked and how to look for answers." (Coombs and Alty, 1984; p. 22)

Computer expert systems, on the other hand, have been developed as problem-solvers in that their sole objective is to achieve known and clearly defined solutions to a well-circumscribed class of problem.

They found that unsatisfactory advisory encounters occurred under several circumstances:

- when the interaction was strongly controlled by the advisor (permitting only a one-way flow of information),
- when users were only required to supply information that could not be obtained elsewhere,
- when no feedback was provided to the user as to how the information was going to be used, and
- when the advisor offered a solution without any justification.

Successful encounters, on the other hand, were found to occur with a fairly experienced user and when the expert and user shared control of the interaction (including problem definition). Each stepped out of their respective domain, and the user became more of an expert by the end of the session. The predominant feature, though, was the explicit verbalization of what was covert and implicit in the unsuccessful encounters. The most favorable strategy was found to be the generation and then critiquing (by both agents) of explanations for some set of problem phenomena in a bottom-up fashion.

### 2.2.2.2. Human-computer advisory interactions

Roth, et al., (1987) conducted a study of the interaction between technicians and an intelligent system designed in the machine-as-prosthesis paradigm (Woods, 1986a) for a troubleshooting application. In this paradigm, the human's role is to serve as the eyes and hands of the machine. The intelligent system in this paradigm typically uses a question and answer dialog as the only means of communication between the human and the intelligent system. The system investigated was developed by an iterative refinement of the rule base by domain experts with the goal being to reduce the skill requirements of the technicians involved in repairing the device. Interaction with the expert system involved directions to the human as to what tests and observations to make and permitted acceptance or rejection of machine's recommendations. They found that, even in static troubleshooting situations where there are not any of the dynamism, safing requirements, and mission impact requirements that occur in aerospace contexts, effective performance required the human to play an active role as a full partner or as a supervisor especially in more complicated situations. The machine-as-prosthesis intelligent system failed to provide any interface mechanisms that supported the technicians as partners in the problem solving process; in other words, the AI system failed to be a team player.

For each of the four diagnostic problems encountered, the investigators were able to trace the canonical path through which the process should proceed. However, this occurred only 20% of the

time due to unexpected variability – underspecified instructions, recovery from errors, adaptation to special conditions, and novel situations. The question and answer format required the operator to remember the data that had been entered and options that existed previously. In addition, it was found that those operators with the most experience and who assumed an active role in the problem solving situation performed significantly better than inexperienced and passive operators. This was due in part to the fact that the serial dialogue required parallel problem solving by the operator to be successful. The human's active role actually amplified the machine expert's ability to cope with unanticipated variability in the world and in the problem solving process.

Based on these results, Roth and Woods (1988) and Woods and Roth (1988b) posed the following challenges in formulating advice:

- what unit or grain of advice is appropriate (should the advisor explain or take over and what is good explanation)? and
- when should the advisor interject (should it be severity dependent)?

### 2.2.3. Towards human-intelligent system cooperation in fault management

While many of the initial expert systems developed were called consultant systems, these intelligent systems possessed minimum capabilities for supporting cooperative interaction with human practitioners. The interaction contained minimal capabilities for explanations of machine solutions and the human domain practitioner had few if any means available to inspect the intelligent system's reasoning or control the system as a resource in his or her own problem solving process. The human team member was required to gather data for the expert system because the expert system was not connected to a database about the state of the device or the monitored process. Similarly, the intelligent system possessed no effector mechanisms and so relied on the domain practitioner to carry out its conclusions about the nature of the fault and how to correct it. However, it was recognized that these systems were not capable of solving all possible problems that might occur; therefore they were called "computer consultants" implying that the human could and should overrule the machine expert whenever he or she determined that it was in error.

The results from Roth, et al., (1987) show that this machine-as-prosthesis form of interaction results in a wall between the human and intelligent system (shown in Figure 4). The active, successful technicians tried to break through this wall to discover the expert system's reasoning process and to manipulate the machine as a resource to help them solve their problem (the human was the problem holder). Thus, the design task in making AI systems team players can be thought of as breaking down that barrier to collaboration or enhancing collaboration by creating effective windows to see through the wall.

The need to integrate human and machine problem solvers into an effective cooperative system – to make AI systems team players – has been recognized, especially for dynamic fault management applications. To do this requires serious consideration of the coupling between human and intelligent system, as well as the requisite interface capabilities, as an integral part of the design of intelligent systems.

Based on results such as those cited in the previous section, it has been realized, especially for applications involving supervisory control of dynamic processes, that a more meaningful interaction between human and intelligent machine was required. As a result of this, as well as trends in the spread of interface technology, intelligent systems have been developed with attempts at more sophisticated capabilities to support human interaction that have typically included graphic displays, windowed workstations, and more extensive explanation capabilities.

The realization that more effective support for collaboration was needed drove people working on the AI research agenda to formulate the problem as one in which the machine expert needs to be more intelligent, in the sense that the intelligent system needs to be a better conversationalist. Hence, a relatively large amount of the effort on human-intelligent system cooperation from an AI point of view has been directed at enhancing the machine's natural language capability and enhancing the machine's ability to talk about its own reasoning (cf., the structured bibliography of work on human-intelligent system interaction, Woods, Johannesen, and Potter, 1991).

It is clear that conversational style interactions as the primary form of communication between the human and intelligent system is inadequate for dynamic fault management applications. One characteristic of these types of situations is that communication demands, information processing demands, and decision demands all tend to go up as the severity of the challenges to process integrity



**Human**                                    **Intelligent System**

What are you thinking?  ———▶    Trying to rule out . . .

                                             Give me data

Why do you want that?  ———▶    The presence of "w" will
                                             eliminate "v" from consideration

                                             The most likely suspect is "x"

Oh really?  ◀———
Why do you think it's "x"?  ———▶    If symptoms "y", then "x"

What about "z"?  ———▶    Duh?

**But that doesn't fix it!**                 © 1991, Woods, Potter,
                                             Johannesen, and Holloway
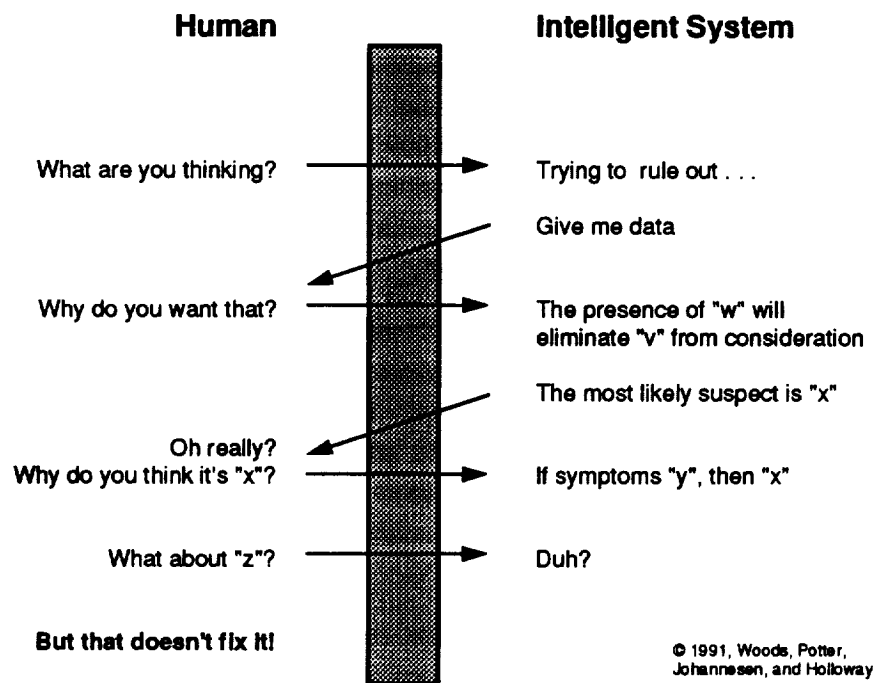
Figure 4.  Interaction across the barrier to human practitioner and intelligent system cooperation in the case of a question and answer dialogue.

go up. The communication bandwidth of a conversational dialogue is too low to support timely and effective exchange of information between cooperating agents under these circumstances (cf. e.g., the results on clumsy automation – Wiener, 1989; Cook, Woods, McColligan, and Howie, 1990; Cook, Woods, and Howie, 1990).

For aerospace fault management applications it is necessary to expand on the model in Figure 4 because the goal of the human operator and the intelligent system is to control/manage a MP. Figure 5 shows a wall between the human and the monitored process. This territory can be addressed in terms of human-computer interaction without any role for intelligent advisory systems. However, the portion of the human-computer interface that is most relevant is concerned with what Woods (1991) calls design for information extraction in HCI – in other words, how does the computer interface help the human operator understand what is going on in the MP.

The introduction of an IS added a new player to the picture. This creates new coordination tasks as the human has to understand what his partner, the intelligent system, is thinking or doing (see Figure
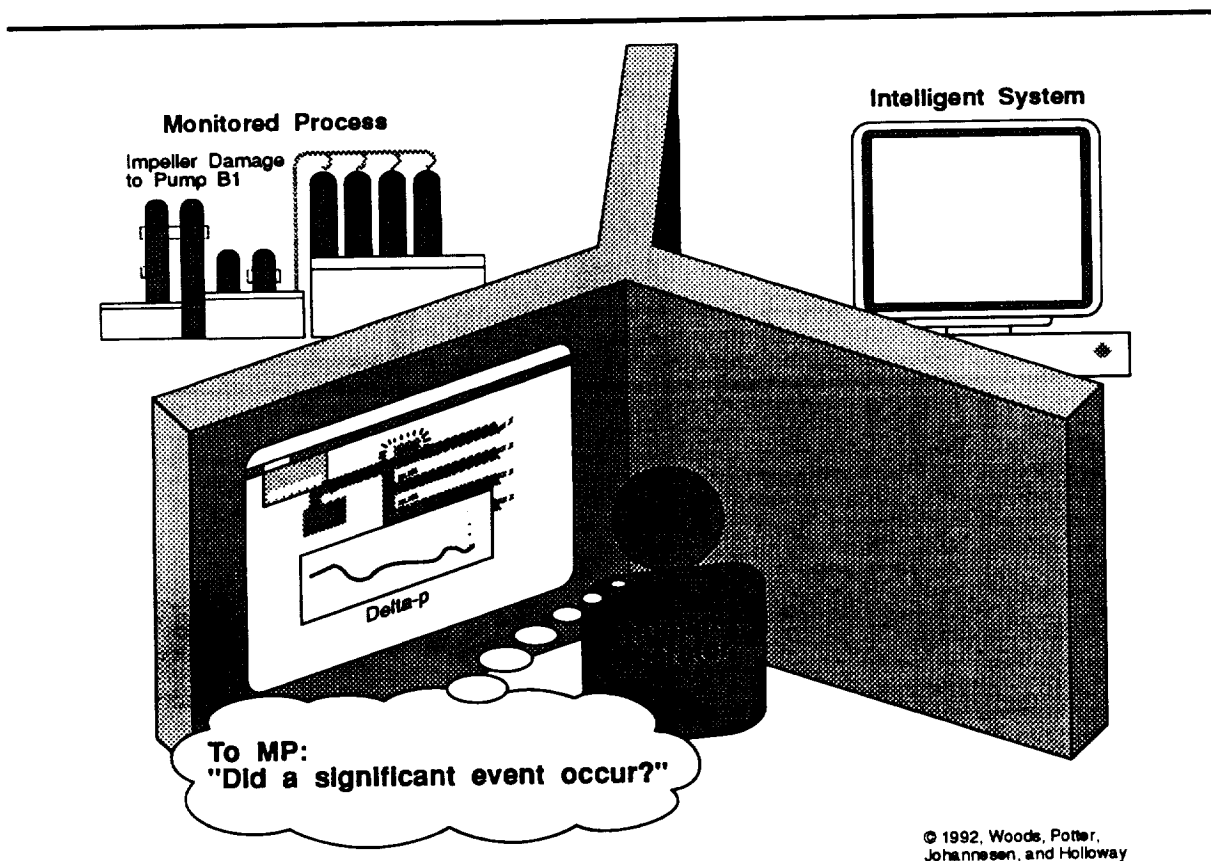


Figure 5. Expanded view of the communication barriers for dynamic fault management applications. In this case the human operator is trying to recognize and track significant changes in the monitored process.

6). But it is important to keep in mind that the ultimate purpose of the human operator (and the intelligent system) in fault management is to track what is going on in the monitored process, recognizing and correcting anomalies.

Figure 5 shows a situation where an event, a change, has occurred in the monitored process. The window available to the human operator (the representation of the monitored process; cf., Woods, 1991) is a kind of display which was typical of the systems examined in the case study phase of this research – a schematic of the physical topography of some part of the monitored process where the active state is represented by digital values. The user's cognitive task is recognizing if a significant event occurred. The representation of the monitored process affects the ability of the operator to do this.

Figure 6 illustrates the collaboration between the human and intelligent system for this hypothetical scenario. The collaboration is influenced by the kinds of representational windows available to assess the intelligent system's view of the situation. It was found that typically there is some kind of message list or menu of options for the kinds of messages or other displays that can be viewed. The
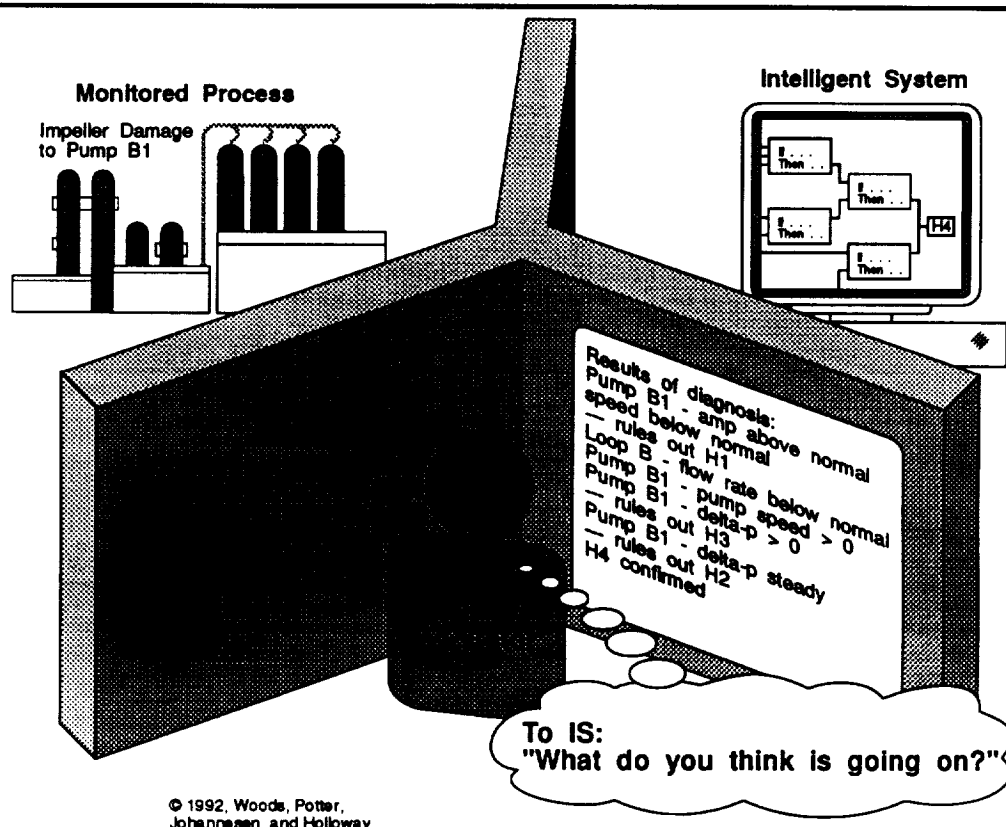


Figure 6. Continued communication barriers for dynamic fault management applications. In this case the human operator is trying to collaborate with the intelligent system in situation assessment.

human must interpret these displays, decide on where additional information may be available within the computer workspace, remember how to get there, examine and integrate the data in order to understand the intelligent system's situation assessment, what faults are present, what corrective actions might need to be taken, what safing actions need to be taken as well as trying to understand how the state of the monitored process is changing. Again, the representation of the intelligent system available to the operator affects his or her ability to collaborate with the intelligent system.

The example explored in Figures 5 and 6 shows how designers can inadvertently reinforce barriers that make it difficult to see what the intelligent system is thinking about or what the intelligent system thinks is going on in the monitored process or to see the flow of events in the monitored process. This points to one of the major themes of this work – visualization. After a description of the specific application investigated in this effort (Chapter 3), the next three chapters will be devoted to developing tools to improve the human operator's ability to visualize the behavior of the MP and track the IS's activity in response to this behavior.

# 3. THE RESEARCH APPLICATION – THERMAL CONTROL SYSTEM

## 3.1. General description

### 3.1.1. Overview

As mentioned in Chapter 1, the application domain is NASA Space Station Freedom's (SSF) Thermal Control System (TCS), being designed to maintain thermal conditions within SSF crew and experimental quarters and to reject excessive heat into space. The purpose of this chapter is to discuss in some detail the functionality of the system and a description of each of the components, focusing on critical parameters and relationships for each. This chapter will end with several scenario-based descriptions of system behavior.

One of the primary system requirements is the ability to adjust internal conditions and efficiency of heat rejection to balance widely varying heat loads imposed (as activities and experiments change). The TCS accomplishes this goal by the use of three main subsystems – a set of evaporators, pumping and control components, and a set of space radiators (or condensers). Figure 7 provides a depiction of a generic configuration; see Chapter 5 for a schematic of the current configuration. At a functional level, one can think of the TCS as two thermal loops (an evaporator loop and a condenser loop) for heat acquisition and rejection, respectively, and a transport loop for pumping and maintaining temperature/pressure equilibrium and inventory control. The following sections will discuss these two functional aspects of the system before going into a more detailed discussion.

### 3.1.2. Heat acquisition and rejection

Heat is acquired into the TCS through a series of heat exchangers (connected in parallel) which transfer heat to the TCS from habitation and laboratory modules and truss mounted equipment where heat dissipation rates are too high to be controlled passively. Liquid ammonia flows into the evaporators, acquires heat, and changes into a wet vapor form (two-phase). One of the key elements of this heat exchange process is the fact that the heat energy is acquired through evaporation, not through temperature change of the medium. Except for the fact that the liquid may enter the evaporators slightly subcooled (a few degrees below saturation condition), the input and output temperature of the ammonia should be the same.

Heat rejection occurs by vapor being pumped through another series of heat exchangers which, by their exposure to space, function as radiators. Within this process, the vapor is condensed back into a liquid form (and also further cooled to a subcooled temperature). Flow rate to the condensers is varied according to the heat load being applied to the system. As heat load increases, flow rate to the condensers increases to increase the amount of heat being rejected. This is due to the fact that heat

24

gained/lost in a heat exchanger is a function of flow rate (which is directly proportional to pressure) and temperature differential.

### 3.1.3. Transport and temperature control

The central device in the TCS is the rotary fluid management device (RFMD), which performs several functions. First, it separates liquid from vapor (the two-phase return from the evaporators) by centrifugal force generated by rotation of the RFMD drum. Second, this rotation produces a pressure differential to maintain adequate flow rates throughout the system. Third, it recombines cold liquid return (from the condensers) with the saturated liquid/vapor combination (from the evaporators). Fourth, it traps and vents non-condensable gases from the condenser return flow.

As heat load on the TCS fluctuates, the liquid/vapor balance varies as well. However, the RFMD does not have sufficient capacity to accommodate these changes. This is the function of the accumulators. They passively maintain inventory (and pressure) equilibrium within the RFMD by adding and subtracting liquid and vapor based on current conditions (heat load, flow rates, etc.).

A critical aspect of the TCS is the ability to maintain a set temperature within the thermal bus despite
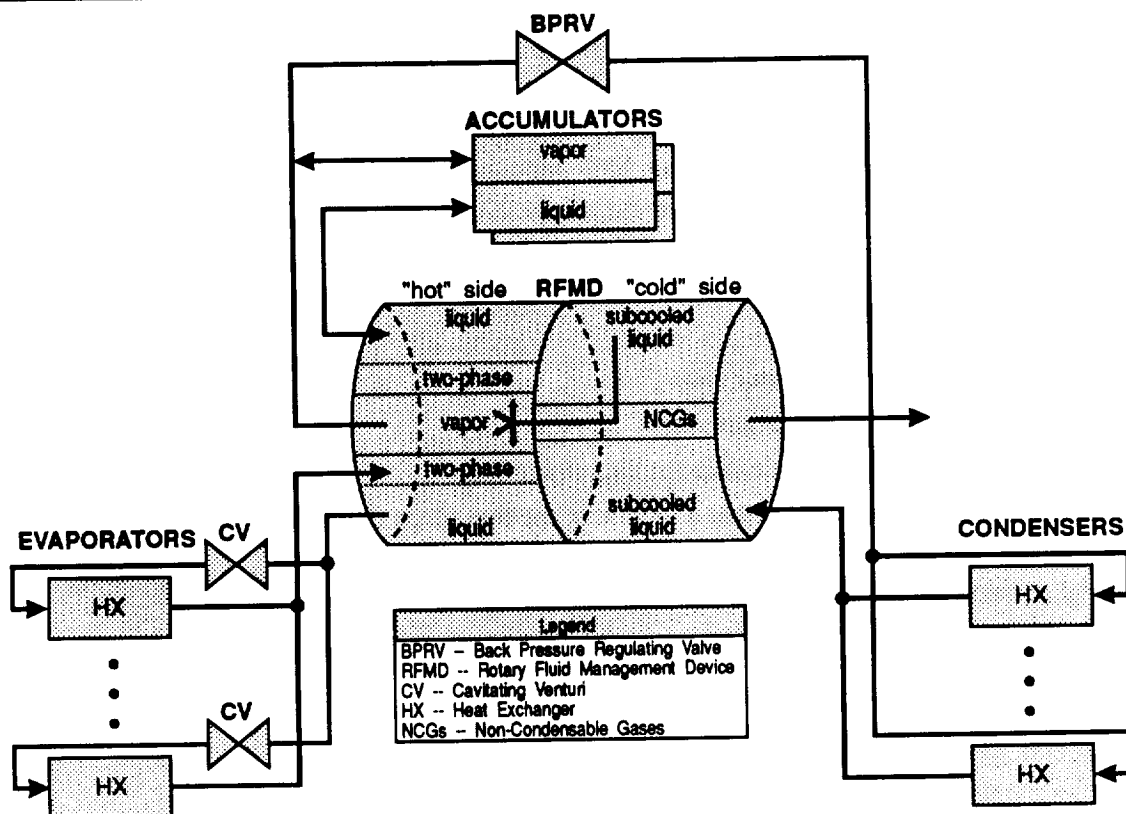


Figure 7. Thermal control system components and functional interconnections.

wide fluctuations in heat load and heat sink applied to the system. This function is performed by the back pressure regulating valve (BPRV), a valve which controls vapor pressure within the RFMD and also the vapor flow rate from the RFMD to the condensers. It accomplishes this by controlling saturation conditions in the main chamber of the RFMD by regulating vapor pressure to maintain the desirable set point temperature of the system (e.g., 70°F). This action in turn varies the pressure (and thus the flow rate) of the vapor to the condensers. As mentioned earlier, higher pressure results in more cooling in the condenser loop, while lower pressure reduces the amount of cooling.

## 3.2. Detailed description of components

### 3.2.1. Evaporators

#### 3.2.1.1. Description

As mentioned above, these are a series of heat exchangers (connected in parallel) which remove heat from the internal thermal control system, transferring it to the external thermal control system. Liquid flows into the evaporators, acquires heat, and changes into a wet vapor form (two-phase).

The critical heat acquisition parameter of exit quality actually can be decomposed into two components. First is the aggregate exit quality of all evaporators after the return lines are recombined. This is important as a global indication of amount of heat being acquired. Second is the exit quality of each individual evaporator (i.e., the maximum of 80% applies to individual as well as aggregate return). It is critical that individual exit quality not exceed the design maximum in order to prevent evaporator overheating. However, the aggregate value may hide important behavior. For example, four evaporators could be yielding 50% exit quality and one yielding 100%, resulting in an aggregate value of less than 80%. Despite the acceptable aggregate value, one evaporator is still in danger of overheating.

#### 3.2.1.2. Critical parameters

- $p_e$ – pressure in the evaporator loop
- $\dot{m}_e$ – flow rate in the evaporator loop
- $\Delta p_e$ – change in pressure across entire evaporator loop
- $\Delta p_{2\phi}$ – change in pressure across a section of the two-phase return line. This is approximately a function of the vapor quality (and thus heat load).
- $\Delta p_{cv}$ – change in pressure across the cavitating venturis

#### 3.2.1.3. Relationships

- $\Delta p_e = \Delta p_{2\phi} + \Delta p_{cv}$

## 3.2.2. Condensers

### 3.2.2.1. Description

Hot vapor flows to the condensers which radiate heat into space. Within this process, the vapor is condensed into a liquid form.

### 3.2.2.2. Critical parameters

- $\dot{m}_c$ – flow rate in the condenser loop. This is also referred to as "condenser return flow".
- $T_{cr}$ – temperature of liquid return at the end of the condenser loop
- $T_{sink}$ – effective temperature to which heat is transferred from thermal bus to space.

### 3.2.2.3. Relationships

- $p_{set}$ and $\dot{m}_c$ should covary together, unless BPRV is opening due to a setpoint change or fault in the system.

## 3.2.3. Rotating fluid management device (RFMD)

### 3.2.3.1. Description

There are two "sides" to the RFMD – hot side and cold side – which are physically separated by thermal barriers. The hot side is the return from the evaporator loop, while the cold side is the return from the condenser loop. Liquid flows from the cold side to the hot side through small holes in the thermal barrier. Also, the cold return is re-saturated by being sprayed into the center of the hot side.

### 3.2.3.2. Critical parameters

- $P_W$ – power (in watts) being delivered to the RFMD
- $N$ – speed of rotation of the RFMD
- $\dot{m}_{bf}$ – bearing flow
- $\Delta p_{end}$ – end-to-end change in pressure. This is the $\Delta p$ around the condenser loop (saturated pressure vs. cold pressure).
- $\Delta p_{evap}$ – pumphead. This is the $\Delta p$ around the evaporator loop

### 3.2.3.3. Relationships

There is a complex relationship between $P_W$ and $N$. For example, much power is required to increase the speed, but once a speed is reached, the power requirement decreases (due to momentum). Also, power can be reduced for up to 30 seconds before speed of rotation will be affected.

### 3.2.4. Accumulators

#### 3.2.4.1. Description

As heat load changes, changes in the liquid/vapor balance in the RFMD are compensated for by two accumulators. The function of the accumulators is to maintain pressure equilibrium between liquid and vapor within the TCS, based on the two-phase return quality. The accumulators contain a spring-balanced bellows-type device to separate liquid and vapor. As the amount (pressure) of one of the agents increases, pressure is exerted on the bellows, causing an accumulation of that agent, forcing out the other agent until pressure equilibrium is achieved. While by design these accumulators can accommodate a wide range of heat loads, they can also compensate for faults (such as leaks) until all inventory is exhausted.

#### 3.2.4.2. Critical parameters

- $L$ – accumulator level (expressed as % full)
- $\dot{m}_{lp}$ – flow rate (of liquid) from the RFMD to the accumulator

#### 3.2.4.3. Relationships

- $L$ and $\dot{m}_{lp}$ should covary together – as flow rate to the accumulator increases, the level increases.

### 3.2.5. Back pressure regulating valve (BPRV)

#### 3.2.5.1. Description

As previously mentioned, the function of the BPRV is to provide setpoint (temperature) control through regulating upstream vapor pressure. This also controls the vapor flow rate to the condensers.

#### 3.2.5.2. Critical parameters

- $A_{bprv}$ – the amount the valve is opened (or closed).
- $p_{set}$ – pressure in the condenser loop upstream of the BPRV. This is the setpoint pressure.

#### 3.2.5.3. Relationships

- The $A_{bprv}$, along with the flow rate ($\dot{m}_c$) (and fluid density) determines the $\Delta p$ across the valve. The relationship is:

$$\Delta p \approx k \left( \frac{\dot{m}^2}{A^2} \right)$$

## 3.2.6. Cavitating venturis

### 3.2.6.1. Description

As previously mentioned, the cavitating venturis provide constant flow rate specifically tuned to the maximum heat load for each evaporator. The key aspect of these devices is to maintain appropriate inlet/outlet pressure ratio (referred to as flow coefficient) to produce cavitation (vaporization) at their outlet. As long as the flow coefficient does not exceed a criteria of .85, changes in heat load will not alter the flow rate. If flow is maintained constant, then exit quality is only a function of heat load. However, above this limit flow decreases, resulting in an underestimate of exit quality. Events which would cause an increase in this flow coefficient include changes in RFMD (e.g., speed, power, or liquid level), BPRV failure, and leaks in the system.

### 3.2.6.2. Critical parameters

- $fc_{cv}$ – flow coefficient – change in pressure across the cavitating venturis
- $\dot{m}_{evap}$ – flow rate to individual evaporators (based on sizing of the corresponding cavitating venturi inlet).

### 3.2.6.3. Relationships

$$\text{flow coefficient} = \frac{(\text{outlet pressure}) - (\text{saturation pressure})}{(\text{inlet pressure}) - (\text{saturation pressure})}$$

## 3.3. Scenario-based description of system behavior

### 3.3.1. Excessive heat load

#### 3.3.1.1. Isolated

When a single evaporator is heated beyond the designed heat load capacity, this results in vapor outlet quality increasing to 100% and then in superheating since the cavitating venturi is set to provide constant flow to reject the design heat load. However, this overheating from a single evaporator has a minimal effect on the overall operation of the system. When the superheated vapor combines with the two-phase mixture from the other evaporators, the superheated vapor just vaporizes a portion of the liquid of the two-phase return. As long as the system heat load input is less than $(Q_{max})0.8$ (80% is the design vapor quality at $Q_{max}$), the two phase return still has the desired saturated mixture with the setpoint temperature returning to the RFMD.

#### 3.3.1.2. Sudden onset

During conditions involving minimal heat load being applied to the system, the evaporator return is predominately liquid. If a large heat load is suddenly applied to the evaporators at this point, the generated vapor will push the liquid from the evaporators and two-phase return lines into the RFMD. This liquid flow rate into the RFMD can exceed the RFMD liquid level probe's ability to pump to the

accumulator and the RFMD fills with liquid. Because of the mass of this additional volume of liquid in the RFMD, it will lose rotational speed and consume additional power (referred to as flooding). This increased volume of liquid causes an increase in the RFMD liquid pressure and causes the end-to-end Δp to drop. Also, because the servo line to the BPRV is connected to the evaporator line, the increased liquid pressure momentarily closes the BPRV. This causes an increase in system pressure and will stop and can actually reverse the flow of liquid from the condensers to the RFMD, resulting in warm liquid exiting the cold end of the RFMD toward the condensers. As the RFMD pumps excess liquid to the accumulators, conditions will slowly recover to nominal.

### 3.3.1.3. Widespread

When the system heat load is greater than the condenser design capacity, uncondensed vapor flows into the cold end of the RFMD from the condensers. This returning vapor forces the liquid level in the cold end of the drum to open, and causes the end-to-end Δp to drop. This slows the flow in the condenser loop. However, the incoming vapor to the RFMD hot drum is continuously being generated by the over-heated load to the evaporators. This results in a system pressure rise. The rise in pressure condenses the vapor in the cold end of the RFMD and the end-to-end Δp is momentarily established and helps the system pressure to be re-established at the higher setpoint. As this new higher setpoint is approached, the capacity of the condensers is again exceeded, uncondensed vapor returns to the RFMD, and the cycle repeats.

## 3.3.2. Loss of subcooling

### 3.3.2.1. Increased sink temperature

The RFMD needs a minimum of 5 to 10°F subcooling in the liquid returning to the cold end of the RFMD from the condensers to maintain stable system operation. As the sink temperature (external temperature at the condensers) increases, condensate return temperature increases. As subcooling is lost, end-to-end Δp drops, resulting in a setpoint pressure/temperature rise to force the vapor flowing through the condenser loop. If the increase in sink temperature continues, this cycle will repeat.

### 3.3.2.2. Loss of condenser

If a blockage occurs in one condenser, there will be an increased pressure drop (across that condenser) which will lead to a redistribution of vapor flow to the other condenser(s). Loss of a condenser during fully loaded heat load to the evaporators will overload the remaining condenser(s), resulting in uncondensed vapor returning to the RFMD. This results in a loss of end-to-end Δp and setpoint pressure, just as in widespread excessive heat load (Section 3.3.1.3.).

# 4. Tracking Intelligent System Activity: Development of Temporal Information Displays

## 4.1. Informational aspects of intelligent system output

One of the guiding questions in this work is one of how the IS conveys information to the human operator. Without exception, the primary representational window used in the systems investigated in Malin, et al., (1991) to help the human operator track the IS's assessment, recommendations, or actions with regard to the MP is a chronologically ordered message list. Message lists are windows that list events in a textual, alphanumeric string format. Typically each entry is one or two lines long. A time stamp is usually associated with each entry, but cases were observed in which no time stamp was used.

Message lists were found to occur in several different forms in the case studies with a variety of different types of information about the MP (e.g., alarms) as well as the IS activity, including:

- configuration (e.g., modes, changes in system setup),
- IS non-essential activities (e.g., initialization, data transfer, computations),
- description of anomalous conditions within the MP (based on static limits *or* model-based expectations),
- testing (to confirm the previous anomalies),
- diagnoses (including alternatives, confidence levels, priorities),
- control actions (either recommended or automatic), and
- predicted future events.

Table 2 presents a series of messages from one example observed. This series of approximately 90 messages was generated in a matter of minutes (as can be seen from the time stamps) from the nearly simultaneous injection of two faults. The window to view these messages contained 25 lines of text.

Chapter 1 described some of the characteristics of fault management, many of which were concerned with the temporal aspects of the task. The following sections will outline the critical temporal and informational issues related to IS output and discuss the weaknesses of message lists in representing this information for display to the human operator. This information will be used as a basis for design concepts and alternative representations to overcome these limitations.

31

## Table 2. Sample IS output — message list.

00.00:00 Initializing, please wait . . .
00.00:00 SSM/PMAD Interface Started, Mode is
-- Ready
00.00:00 Recomputing Gantt Chart, Please
-- wait . . .
00.00:08 SSM/PMAD Interface Mode is
-- Autonomous
00.00:11 Sending Event List To the LLP's
00.00:11 Sending Priority List to the LLP's
00.00:15 Recomputing Gantt Chart, Please
-- wait . . .
00.00:17 Computing Requested Information,
-- Please wait . . .
00.00:27 Formatting power utilization data . . .
-- please wait
00.01:22 LLP LC-2, switch: 2 tripped on
-- UNDER-VOLTAGE.
00.01:22 LLP LC-2, switch: 3 tripped on
-- UNDER-VOLTAGE.
00.01:22 LLP LC-2, switch: 4 tripped on
-- UNDER-VOLTAGE.
00.01:22 LLP LC-2, switch: 5 tripped on
-- UNDER-VOLTAGE.
00.01:22 LLP LC-2, switch: 6 tripped on
-- UNDER-VOLTAGE.
00.01:22 LLP PORT, switch: P03 tripped on
-- FAST-TRIP.
00.01:22 LLP STARBOARD, switch: S02 tripped
-- on FAST-TRIP.
00.01:22 LLP LC-1, switch: 16 tripped on
-- UNDER-VOLTAGE.
00.01:22 LLP LC-1, switch: 17 tripped on
-- UNDER-VOLTAGE.
00.01:22 LLP LC-1, switch: 18 tripped on
-- UNDER-VOLTAGE.
00.01:22 LLP LC-1, switch: 19 tripped on
-- UNDER-VOLTAGE.
00.01:22 Sending Event List To the LLP's
00.01:22 Opening switches: LLP: PORT, switch:
-- P03 LLP: LC-2, switch: 0 LLP: LC-2, switch:
-- 1 LLP: LC-2, switch: 2 LLP: LC-2, switch: 3
-- LLP: LC-2, switch: 4 LLP: LC-2, switch: 5
-- LLP: LC-2, switch: 6 LLP: LC-2, switch: 7
-- LLP: LC-2, switch: 8
00.01:22 Reclosing switch: LLP PORT, switch:
-- P03

00.01:22 LLP PORT, switch: P03 tripped on
-- FAST-TRIP.
----- 00.01:22 Diagnosis -----
LLP PORT, switch P03 tripped on FAST-TRIP.
During testing LLP PORT, switch P03 retripped
-- on FAST-TRIP.
POSSIBLE CAUSES:
Most Likely:
Low impedance short in cable below switch,
-- switch output of switch, or the
switch input of one of the lower switches.
Less Likely:
Current sensor in switch reading high.
------------------------------------------
Opening switches: LLP: STARBOARD, switch:
-- S02 LLP: LC-1, switch: 14 LLP: LC-1, switch:
-- 15 LLP: LC-1, switch: 16 LLP: LC-3, switch: 17
-- LLP: LC-1, switch: 18 LLP: LC-1, switch: 19
-- LLP: LC-1, switch: 20 LLP: LC-1, switch: 21
-- LLP: LC-1, switch: 22
00.01:23 Reclosing switch: LLP STARBOARD,
-- switch: S02
00.01:23 LLP STARBOARD, switch: S02 tripped
-- on FAST-TRIP.
----- 00.01:23 Diagnosis -----
LLP STARBOARD, switch S02 tripped on
-- FAST-TRIP.
During testing LLP STARBOARD, switch S02
-- retripped on FAST-TRIP.
POSSIBLE CAUSES:
Most Likely:
Low impedance short in cable below switch,
-- switch output of switch, or the
switch input of one of the lower switches.
Less Likely:
Current sensor in switch reading high.
------------------------------------------
Sending Event List To the LLP's
00.01:24 Sending Priority List To the LLP's
00.01:30 Recomputing Gantt Chart, Please
-- wait . . .
00.01:30 Computing Requested Information,
-- Please wait . . .
00.01:30 Computing Requested Information,
-- Please wait . . .

## 4.2. Temporal sequence and density

### 4.2.1. Problem description

One of the primary features of the example in Table 2 is that there are no distinguishing features to the messages to give any indication as to the temporal sequence of the message. Each message is simply written below the previous one, resulting in the appearance a continuous stream of entries, hiding the underlying temporal structure. This creates a "packed" representation that obscures the temporal distances between events. One cannot see at a glance whether events occurred contiguously or farther apart. This is accomplished only through reading and comparing time stamps. This problem is demonstrated in a simple comparison of the two hypothetical message lists illustrated in panels A and B of Figure 8. The same events occur in the same order in the two panels. However, the time stamps are not sufficient to make the pattern of temporal relationships stand out. By indicating events against an analog timeline, panels C and D of this figure immediately reveal the pattern.

Depicting temporal sequences is important from two perspectives. First, it is important to address questions such as:

* how long since the last message?
* how much activity has there been recently?

**MESSAGE LIST VS. TIMELINE INFORMATION DISPLAY FOR TWO SAMPLE CASES**

**A.**

```
10:23:43 Switch 3 tripped
10:31:07 Switch 4 tripped
10:32:23 Load Shed
```

**B.**

```
10:23:43 Switch 3 tripped
10:24:27 Switch 4 tripped
10:32:23 Load Shed
```

**C.**
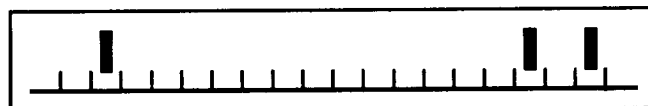
**D.**
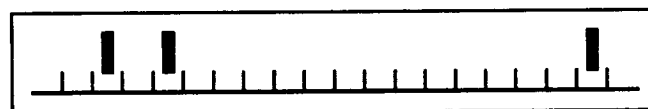
© 1991, Woods, Potter, Johannesen, and Holloway

Figure 8. An example of a sequence of events illustrating how message lists obscure information about the temporal distance between events.

- how long ago was all that activity?

- does this particular group of messages represent a flurry of activity in the recent past, or a description of what has happened over the last hour (with many periods of inactivity)?

Second is the temporal characteristics of the MP, such as modes, phases, etc. that need to be represented through the operator interface. Third is the issue of temporal sequence playing a role in diagnosis. These latter two issues will be discussed in subsequent sections of this chapter.

### 4.2.2. Design concept(s)

(1) Information within a message list should be spatially organized to depict temporal patterns and sequences.

### 4.2.3. Alternative representation(s)

One type of temporally organized display is a timeline where an analog representation of time is used as the organizing anchor to represent sequences of events. Timeline formats have been used in the past to represent plans, for example, the planned sequence of events in a startup, launch, landing, or docking sequence. These are plan-based, rather than the event-based characteristics of a message list.

Additionally, timeline displays have been used in scheduling aircraft for air traffic control (ATC) displays (Seagull, 1990). Figure 9 presents a comparison of two types of displays for ATC operations in which minimum separation distance is the critical parameter. This example shows the obvious superiority of a timeline display for this type of task – no one would think of using the impoverished representation of a message list for this type of application. In the timeline display, warnings and recommended actions can be integrated into the display in a manner that is consistent with the operator's cognitive task (Roth and Woods, 1989).

## 4.3. Temporally fleeting data

### 4.3.1. Problem description

Another feature of the example in Table 2 is that each entry in the window is a line or lines of text. Because of this, when a series of events occurs, the list of messages can quickly exceed the space available in the viewport (as seen in Figure 10), creating a *keyhole effect* (Woods, 1984). This forces the operator to read and scroll through several screens of messages to find inter-related messages and to "piece together" a global view of what is happening with the process, the pattern of automatic actions, and the intelligent system's assessment or recommended actions.

This figure provides an example of how relationships between messages can be very difficult to extract. The gray region shows the full message list. The window overlay contains a smaller viewport with only a portion of the list in view. Messages concerning Switch 1 ("Switch 1 tripped" is referred to as "Anomaly 1") have scrolled out of view. The message that Switch 2 has tripped is displayed followed by the diagnostic message, "Recommended actions for Anomaly 1: manually re-route to lower circuit". Because a portion of the list is hidden and because of the poor wording of the

messages, this and the other diagnostic messages seem to be referring to the Switch 2 event when they are actually referring to the Switch 1 event. The message list makes it difficult to establish the context for each message "at a glance."

While messages typically include time stamps, these do not help the operator quickly apprehend temporal information; each message and time stamp must be read and compared to other messages. Furthermore, as one scrolls around in a long message list it is easy to get lost as the packed textual field contains no readily apparent temporal *landmarks* (Woods, 1984) (e.g., current time is rarely highlighted on the message list displays surveyed in Woods, et al., 1991).

### *4.3.2. Design concept(s)*

(2) Link events to an overview timeline display to provide a macro view.

    (a) Need to indicate current time.

    (b) Need to highlight messages being displayed (if not current).



Figure 9. A comparison of message list and timeline formats for an ATC display designed to schedule aircraft arrivals (the left panel is adapted from Seagull, 1990).

## 4.3.3. Alternative representation(s)

Implementation of an overview timeline display in parallel with a temporally organized message list should provide complementary views into the sequence of events presented. The overview timeline should present a depiction of event occurrence and density in order to provide cues as to the location of events not displayed within the message window.

Several questions arise at this point, including:

- **How are the two views coordinated?** There would need to be an indication on the overview timeline as to where the message list is scrolled. In essence, the overview timeline should behave as an enhanced scroll bar, depicting where events are located in time, where the current view is positioned, and how much of the total space is displayed.

- **What provisions are there to make sure that new messages are not missed (while scrolling back through previous messages)?** Several approaches are possible: 1) a new message is represented by a new indication on the overview timeline, 2) the window is immediately and automatically scrolled to the bottom when a new message arrives, and 3) provide two windows to view messages. New messages are posted in the current window and do not affect the past window.

The example in Figure 11 demonstrates the use of an overview timeline display to depict temporal



**COMPLETE MESSAGE LIST VS.
PARTIAL MESSAGE LIST WINDOW**

Running operational sequence A (13:34:23)
Control switch 1 tripped (13:36:42)
Beginning automatic diagnostics (13:36:43)
Finishing automatic diagnostics (13:38:44)
Results of diagnostics (13:38:29)
    Failure to uplink to lower circuit
Attempting to correct (13:38:33)

Correction sequence failed (13:40:03)
Switch 2 tripped (13:40:19)
Beginning automatic diagnostics (13:40:20)
Recommended actions for Anomaly 1: (13:40:23)
    Manually reroute to lower circuit
    Failure to respond may cause loss of main power flow
Finishing automatic diagnostics (13:40:22)
Results of diagnostics: (13:41:37)
    Switch 2 tripped on fast trip
    Operator must reroute to continue operational

sequence A
    Failure to respond could cause system shut down

© 1991, Potter and Woods

Figure 10. Partial message list window overlaid onto the complete list of messages. Some of the messages have 'scrolled away,' forcing the operator to scroll through the information in the window.

and density information about past events. In this approach, two windows – "current" and "past" views – are used for posting new messages and scrolling back to review past messages, respectively. Coding of events on the timeline is based on a histogram approach. The number of events within a given time period are represented by the width of the tick mark. In this scenario, the "past" window has been scrolled back to a period of activity.

## 4.4. Temporal characteristics of the physical system

### 4.4.1. Problem description

In most systems, there are known phases, states, modes, and durations which govern the temporal nature of the state transitions. For example, in several of the systems studied, there were events that:

- contained prescribed temporal sequences (i.e., event A cannot occur prior to event B) or time limits for transitions to other events (i.e., event A cannot occur more than x secs. after event B),
- once started, would continue for a certain period of time, and
- were required to be completed at a certain time (i.e., scheduled operations).

These types of events dictate the intrinsic time duration of the MP, including time to complete procedures and time for system changes to take effect throughout the entire MP. Events of this type



© 1994, Scott S. Potter
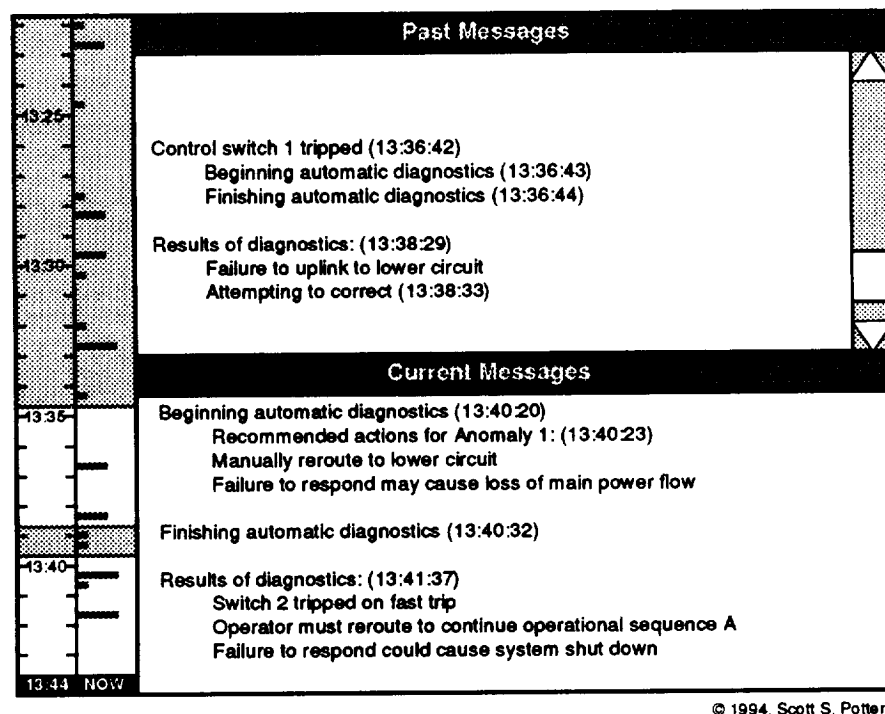
Figure 11. Illustration of an overview timeline display to provide indications of temporal relationships between events (length of tick mark indicates number of messages per time unit).

may be an indication of future behavior or events. For example, an event may be the start of a process of a fixed duration. Therefore, the end of this process is another event which may be informative to the operator before it actually happens. Also, planned future activities may impact the present-state control of the MP. Figure 12 presents a plan-based format which indicates the temporal sequence of past as well as planned future events.

### 4.4.2. Design concept(s)

(3) Display the estimated time of future events on the timeline display.

    (a) This provides an indication of duration of processes (available after initiation).

    (b) Scheduled events may be known before they occur and can be anticipated.

(4) Use messages as one means to indicate change in mode, phase, etc. However, present mode should also be indicated in another, permanently visible manner.

### 4.4.3. Alternative representation(s)

Figure 13 presents a sequence of events for a process consisting of manipulating an apparatus (deploying and stowing) with two redundant motors. The critical aspects of this example are: 1) as soon as the deployment is initiated, the predicted completion time is known (assuming normal operations), 2) as soon as the expected completion time is exceeded, information is gained about system status (i.e., at least one of the motors has failed). Also, a new predicted completion time is generated (based on one remaining motor). As is evident from this example, the predicted information provides context to assist in the understanding of current events.

**TIMELINE FORMATS**

**Event Driven**



Past Events

**Plan Based**
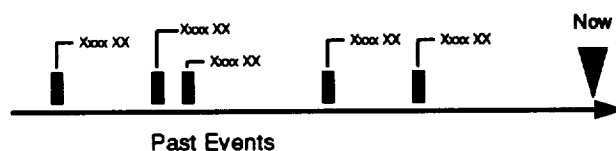


Past Events        Planned Events
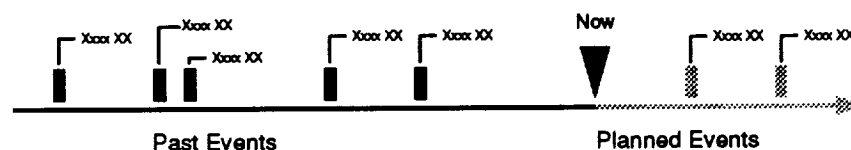
© 1991, Potter and Woods

Figure 12. Above: Event-Driven format to show past events spatio-temporally organized. Below: Plan-Based format to show both past and planned events in a spatio-temporal organization.

## 4.5. Temporal cascade of events

### 4.5.1. Problem description

Qualitative temporal reasoning is an issue that has received considerable attention within artificial intelligence (Decortis, et al., 1991 refer to this as *structure links*). In this approach, the seven possible qualitative relationships with regard to the start and stop times and amount of overlap between two events have been identified. These are illustrated in Table 3. The issue is that there can be dynamic diagnostic reasoning about events based on these temporal sequences (both in terms of machine and human reasoning).

There is a variety of types of temporal patterns that occurs across events in fault management applications. For example (as depicted in Figure 14), an earlier event might be a premonitory sign of later major trouble. Several contiguous events may indicate a single underlying fault. One fault can produce a cascade of disturbances and their associated manifestations which will be seen as a temporally evolving series of events that follow the original burst of activity (Woods, et al., 1986). In this case the diagnostician needs to see the cascade, distinguishing between manifestations that indicate the source of trouble and those that result from disturbance propagation. In addition, one will need to discriminate among independent subsets of events. Finally, the intelligent system may
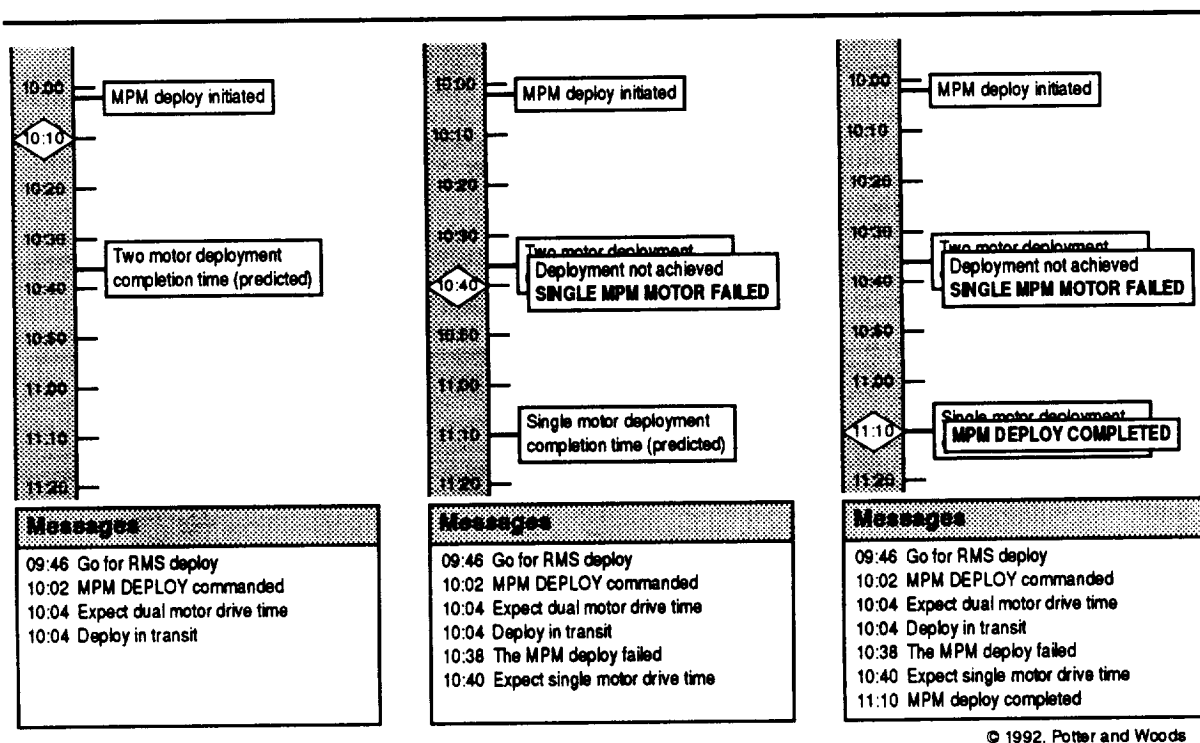


Figure 13. Example showing predicted events being confirmed or disconfirmed. The three panels are snapshots in time of a sequence of events.

produce commentary about the events in the monitored process that are linked to different subsets of the event sequence. These temporal patterns in event sequences are not readily apparent from a message list.

## 4.5.2. Design concept(s)
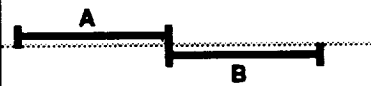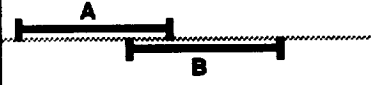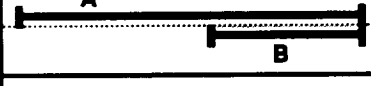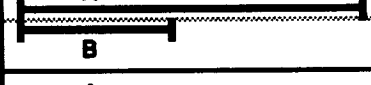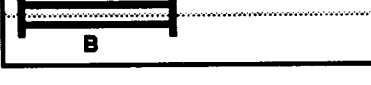
(5) Link IS information to event(s), not timeline.

(a) The key is to integrate MP events and IS activity.

(b) IS activity is in response to MP events. Therefore, it is important to link it to the precipitating events. This will help establish mapping (one-to-one, many-to-one, one-to-many) between events and diagnoses.

## 4.5.3. Alternative representation(s)

The primary question in designing a more useful representation for the intelligent system's output is what information does the operator require to achieve his goals. Message lists are typically used for several purposes, including:

- to convey any change in the state of the monitored process (events such as parameter change, change in mode, goal completion, etc.),

- to indicate intelligent system situation assessment (diagnosis), and

Table 3. Qualitative relationships between events.

| Temporal Relationship | Description in terms of A | Description in terms of B |
|---|---|---|
| A / B | Before – A is before B and they do not overlap | After – B is after A and they do not overlap |
| A / B | Meets – A is before B and there is no interval between them, i.e., A ends where B starts | Met by – B is after A and there is no interval between them, i.e., B begins where A ends |
| A / B | Overlaps – A starts before B starts and they overlap | Overlapped by – B starts after A starts but before A ends, A ends before B ends |
| A / B | Contains – A starts before B starts and ends after B ends, i.e., A contains B | During – B starts after A starts and ends before A ends, i.e., B occurs during A |
| A / B | Ended by – A starts before B starts and they end concurrently | Ends – B starts after A starts and they end concurrently |
| A / B | Started by – A and B start simultaneously and A ends after B ends | Starts – B starts simultaneously with A and ends before A ends |
| A / B | Equal – A and B have the same interval | Equal – B and A have the same interval |

- to provide recommended actions or control actions taken (possibly with an explanation).

Based on these purposes, the following organizations have been developed.

### 4.5.3.1. Anomaly-hypothesis organization

In fault management, many times there are several hypotheses that the intelligent system investigates in diagnosing a fault. If this is the case, it would be advantageous to indicate this to the operator. Figure 15 presents a before-after example adapted from Johns (1990) in which an anomaly triggers four hypotheses which must be tested and/or eliminated. In each panel of the figure, several intermediate steps have occurred (fault detection, hypothesis generation, iterative hypothesis elimination), while only the final display configuration is presented.

This representation eliminates the need for the operator to read through the inter-related messages in order to construct a high-level understanding of the state of the monitored process and the intelligent system's situation assessment. As the intelligent reasoning progresses, the status indicators would change from "UNCONFIRMED" to either "NO" or "YES" to indicate results of testing. Use of graphic annotation and highlighting reduces the burden of identifying test results. It is important to note that this approach gives the operator a sense of what the intelligent system is doing and what will happen next.
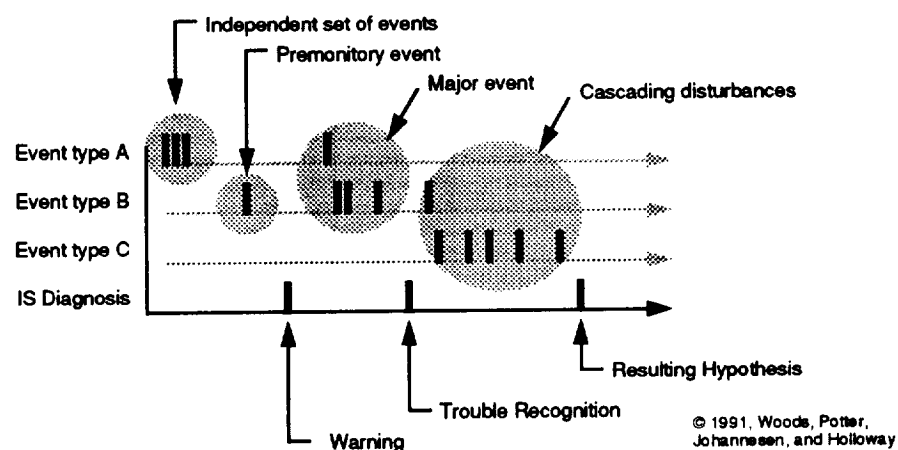


Figure 14. Above: sequence of events spatially displayed on a timeline to convey temporal relationships. Below: event-type categorization added to spatio-temporal information to portray patterns of events.

## 4.5.3.2. Event driven timeline displays

As indicated in the previous figures, a message list is typically made up of different *types* of messages. However, the message lists surveyed generally did not distinguish between message categories. While one intelligent system surveyed did try to categorize messages by placing different types into different message list windows, the lack of indication of temporal interval and the packing of messages removed any anchor for comparison across windows. Furthermore, the workspace design provided the user with window placement flexibility creating the opportunity for misalignment of the related windows. (Actually, in this case it may be even more misleading to align the windows since there is no necessary temporal ordering relation maintained across the windows.)

Figure 16 demonstrates a potential application of an event driven timeline display as an alternative approach to organize the same sequence of events presented in Figure 10. This representation spatially segregates messages based on a top level categorization of events/automatic actions, intelligent system diagnostics, and recommended responses. Within this categorization, the sequence of events distinguishes the two anomalies. Note that the critical features of the previous examples are integrated in this design.

The combination of analog timeline and categorization of messages reveals the pattern of relationships in the sequence of events and greatly enhances an observer's ability to track monitored process behavior and intelligent system assessment/actions. It is important to understand that there are two

**TYPICAL MESSAGE LIST FORMAT**

**ANOMALY-HYPOTHESIS FORMAT**



© 1991, Potter and Woods
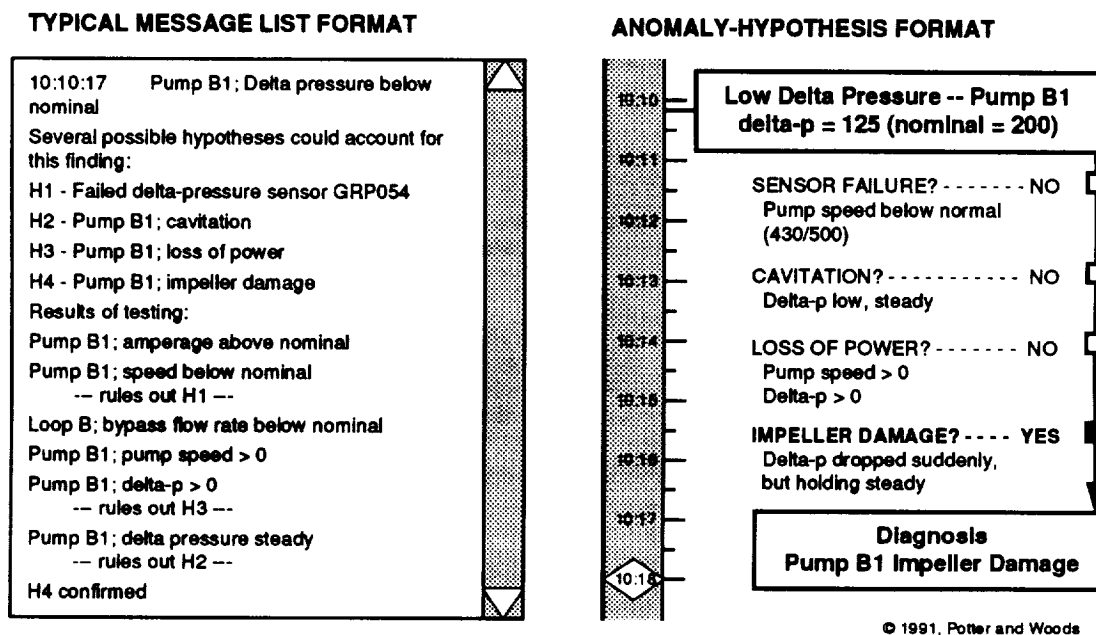
Figure 15. Comparison of typical message list format for output from an intelligent system and anomaly-hypothesis format for a hypothetical scenario (the right panel of the figure is adapted from Johns (1990).

directions of relationships that need to be captured. First, an anomaly triggers intelligent system diagnostic responses (e.g., Figure 15). Second, there are cases in which intelligent system assessments must be linked to the events that are explained (as well as to the events that are not explained). Both of these relationships are represented through an event driven timeline display.

## 4.6. Information overload (granularity problem)

### 4.6.1. Problem description

One central problem throughout all of the examples in this chapter (and in message lists in general) is the problem of the large number of available messages (available information) compared to the smaller number of critical messages (relevant information). This results in the problem of having to read all of the messages in order to locate the critical one(s). While the approach in Figure 16 certainly imposes an organizational structure to assist in this process, there still may be considerable filtering of irrelevant messages required to visualize the MP events and the related IS activity.

There are two aspects to this problem. The first will be referred to as the "time/space" problem. The basic conflict arises from using vertical space as temporal units (as in the overview timeline display) and also as information (since each message consists of one or more lines of text). A flurry of
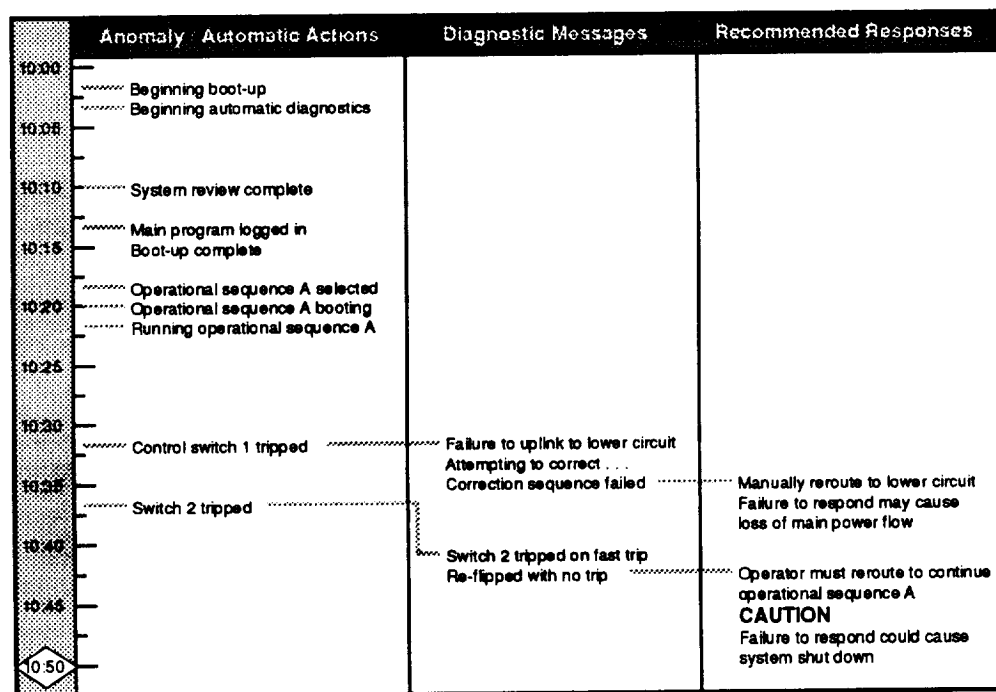


© 1991, Woods, Potter, Johannesen, and Holloway

Figure 16. An example of an event driven timeline display which categorizes intelligent system messages by type (automatic action, diagnostic message, or recommended action) and by temporal sequence.

activity producing many messages can result in more information than allocated space. While one approach is to simply set the time scale fine enough so that a group of messages will not extend past the assigned temporal unit, this is not practical a priori due to the asynchronous nature of events and activity. However, it does appear to be true that the granularity of the time unit will depend on the application – in some cases events tend to occur much more quickly than in others (e.g., electrical vs. thermodynamic systems) and thus require a finer resolution of the time scale.

The second aspect concerns the organizational structure of the messages. This is particularly relevant for the situation discussed in the previous section in which many MP events have occurred, a subset of which have resulted in a diagnosis by the IS. In this case it is important to (1) indicate the relationships between MP events and related IS diagnosis (as in Figure 16), and (2) segregate the essential MP events from the non-essential ones. Both of these may be accomplished by coding the precipitating events and the resultant diagnosis to indicate the causal relationships, as discussed below.

### 4.6.2. Design concept(s)

(6) Provide a means for manipulating the "field of view" of messages. This can be accomplished by either:

    (a) filtering non-essential messages, or

    (b) highlighting essential ones.

### 4.6.3. Alternative representation(s)

There are two approaches to the time/space problem:

- **Fixed time unit.** Allocating each temporal unit $x$ number of lines within the message list. If more than $x$ messages occur during that period, some sort of filtering must take place. If no messages are posted within the given time interval, a blank line is added.

- **Variable time unit.** Permitting each temporal unit to vary depending on the number of messages present. While this has the problem of failing to maintain temporal distance, it has the advantage of displaying all messages.

The primary trade-off between these two approaches is the difference in "field of view". In the variable time unit approach, the amount of time displayed in the window depends on the number of messages that have been posted, while in the fixed time unit approach a given amount of time is always presented (see Figure 17). It is important to note that the variable time unit approach presented in this figure (illustrated on the bottom portion of the figure) has compressed the information by allocating less space to time units with no activity. This permits the depiction of temporal sequence yet also makes more efficient use of available space.

Within a filtering approach, the key is to develop an organizational structure to permit "zooming" in and out by hiding lower level messages and thus presenting (and highlighting) only relevant, critical ones (see Figure 18). As messages are suppressed, a wider field of view can be presented. This can be accomplished by either a rank ordering scheme or a classification scheme (or a combination of the

two). A useful analogy to the rank ordering scheme is outlining features in current word processing systems. Each level in the outline would correspond to a different level or type of message. Selections can be made as to how far down into the outline to present, suppressing lower levels. It is important to note that this approach does not attempt to select *the* most important datum; rather to structure and bound the relevant data set. This reduces the probability of suppressing important information and increases the robustness of the system to different situations.

To address the problem of linking MP events and IS activity, the key is to highlight essential messages in order to bring them into the foreground against the background of the non-essential messages. However, this does not necessarily address the problem of field of view (time/space problem). It primarily deals with an organizational structure to enhance the information extraction properties of the display. The highlighted messages can refer to one event or one diagnosis and serve to segregate relevant from extraneous messages. One strategy for accomplishing this would be to highlight those messages relevant to the antecedent conditions of the rule (in a rule-based IS) which fired to produce the diagnosis. This approach could, however, be linked with a filtering strategy to not only highlight relevant messages but also reduce the amount of messages presented. This would impose additional constraints on the classification scheme (i.e., a message may become more critical when it is a
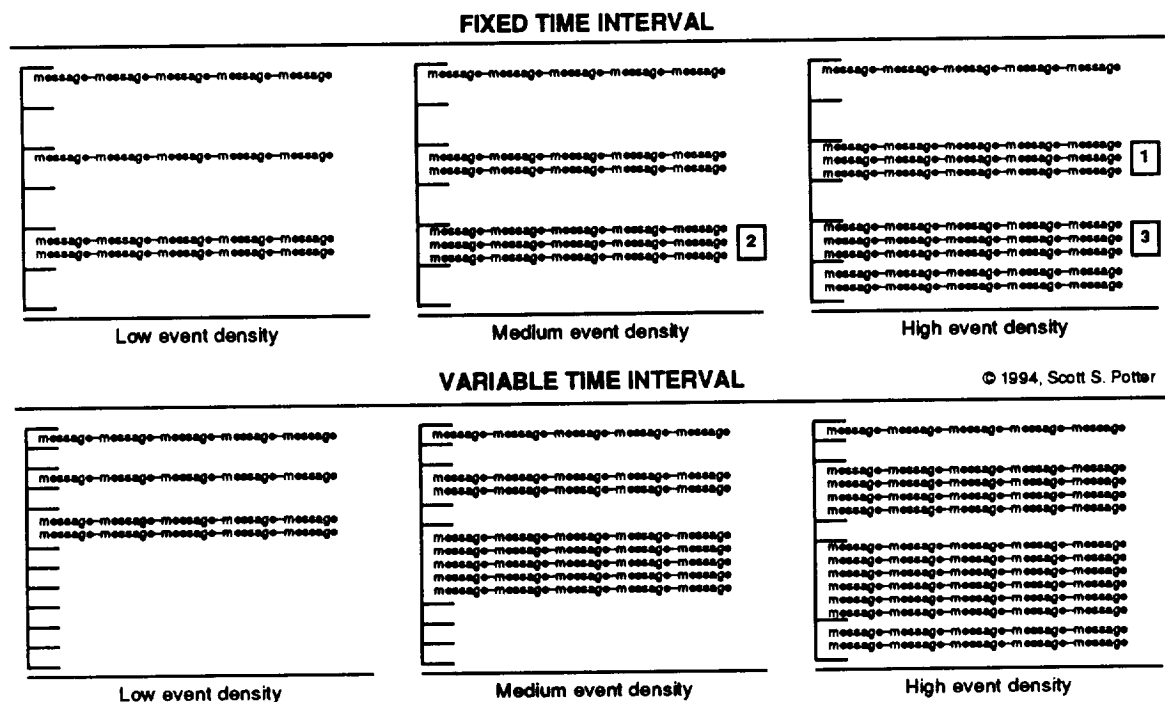


Figure 17. Top: Fixed time unit message list. As more messages occur, filtering is required to maintain consistency in time units. Number to right of messages indicates suppressed messages. Bottom: Variable time unit message list. As messages become denser, temporal units vary to accommodate all messages.

contributory factor to a diagnosis).

A similar organizational structure can also be used on the overview timeline display to provide additional information concerning the types of messages and their temporal sequence. This would allow not just landmarks as to the temporal sequence and density of events, but some degree of informational content as well. For example, IS diagnoses could be highlighted on the timeline display to depict where anomalies occurred which resulted in a diagnosis. This would assist in distinguishing anomalous from nominal activity. The use of highlighting is demonstrated in Figure 19. In this figure, criticality of messages is depicted on the overview timeline display by length and darkness of the tick marks. In this manner, the most critical message for a given temporal unit is always indicated. Within the messages, all messages related to "control switch 1 tripped" are highlighted (bold and italics) to aid in distinguishing between the different sources of the IS messages.

The primary issue addressed in these examples is providing a means for managing the abundance of potentially informative messages about MP behavior and IS activity. The specific representations provide attempts to achieve this goal; however, other approaches could also be developed to accomplish the same goal. For example, much work has been done on alarm prioritization and filtering within nuclear power plants (e.g., O'Hara and Brown, 1991; Lupton, Lapointe, and Guo, 1992).
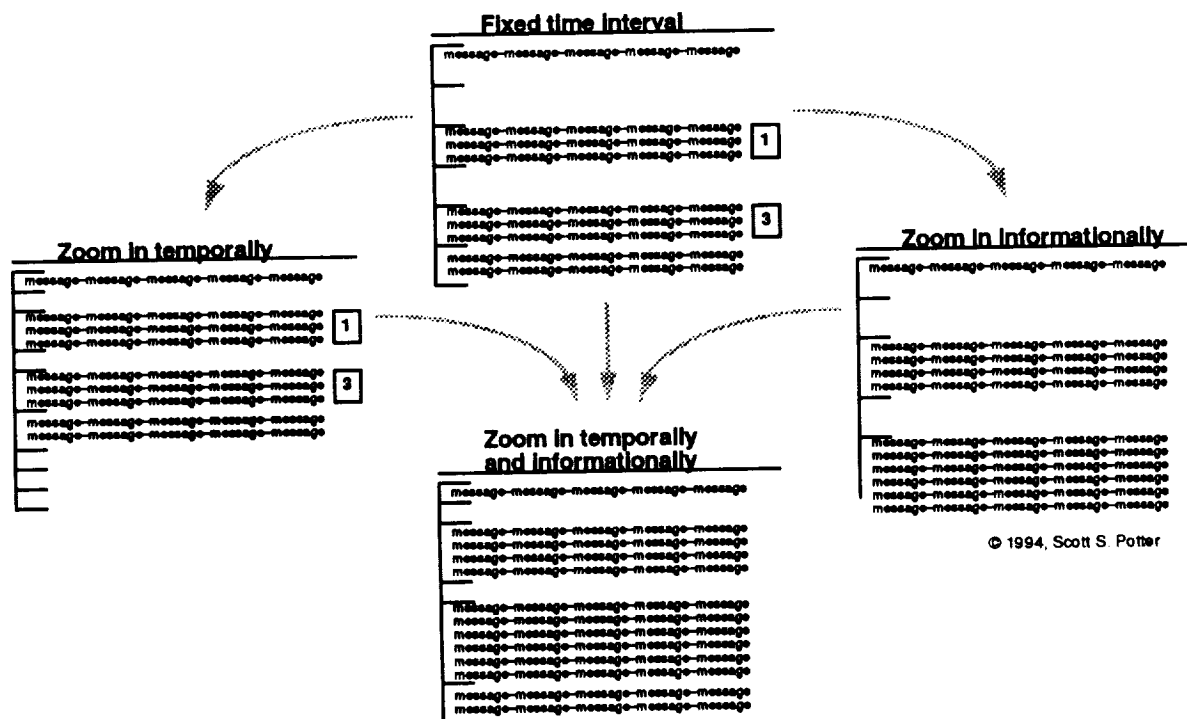


Figure 18. Illustration of temporal and informational "zooming in" within a temporally-based message list.

While little has been included herein on specifics of a classification scheme, this is one area that would require substantial additional attention within a complete design.

## 4.7. Informational properties of text messages

### 4.7.1. Problem description

As is evident from Table 2, another issue to be addressed is the linguistic properties of alphanumeric messages. In most applications of message lists, there were no standard templates or structure to which messages conformed that would aid information extraction. Human operators are forced to deliberatively read all of the messages and assess the relevance of each to the current context. However, given the abundance of messages, it is more likely that the operator will be scanning through the messages trying to construct an understanding of the situation and then, secondarily, ascertaining the significance of individual events to the current context (to confirm or disconfirm current hypothesis). Thus the key is to provide mechanisms for rapid situation assessment (along the same lines of the design goals of the 'status-at-a-glance' display – see Potter, et al., 1992 and Chapter 5) to enhance this process.

In one respect, this is similar to the organizational problem discussed in the previous section in that
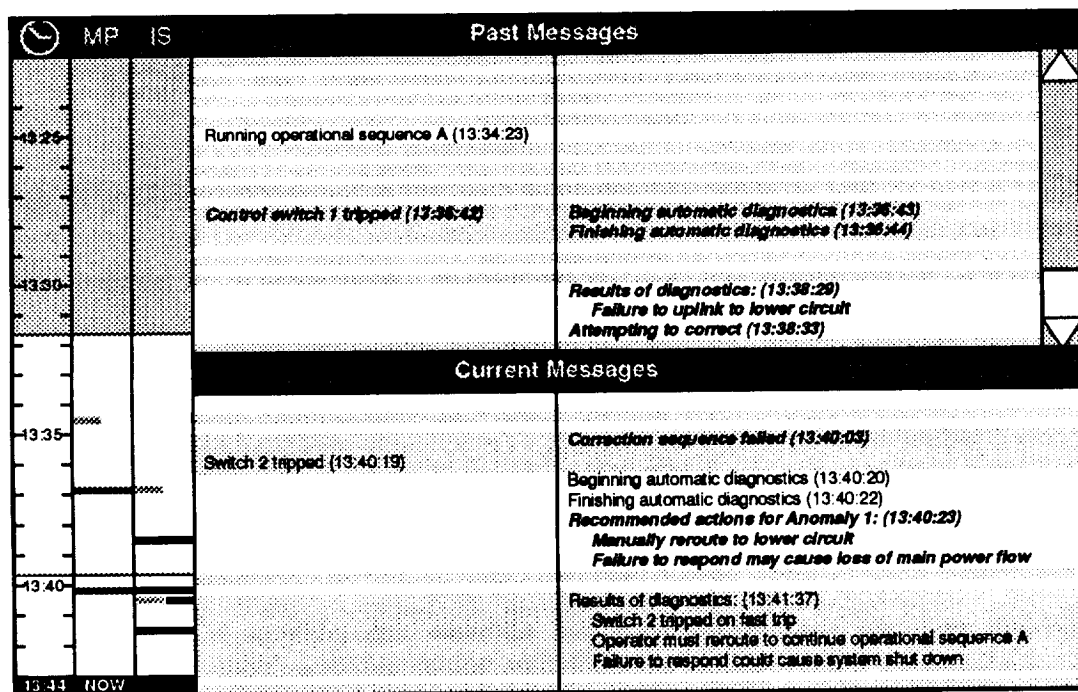
Figure 19. An illustration of highlighting messages to group related information. In addition, coding of the timeline display corresponds to message type (see text for details). Shading of message list illustrates the use of variable time interval.

(a) highlighting related messages (as in Figure 19) should also assist the construction of situation assessment through emphasizing cause and effect relationships and (b) the form and content of the message should aid discrimination of message criticality (and thus reduce data overload). At a deeper level, though, the objective should be to communicate what has changed (or may be about to change) rather than being state-oriented (value of the parameter in question). The form and content should provide (at a glance) information about the components and/or functions affected and the functional impact of the anomaly (to assist in the disturbance management cognitive task discussed in Chapter 2).

## 4.7.2. Design concept(s)

(7) Provide structure and organization within the messages to facilitate rapid situation assessment through:

   (a) high-level depiction of behavior, activity, and criticality,

   (b) standard structure for all messages, and

   (c) providing appropriate context in which to evaluate the information.

## 4.7.3. Alternative representation(s)

The example previously presented in Figure 15 provides a demonstration of these concepts. The "before" design illustrates several deficiencies, including:

- lack of quantitative data ("pump speed below nominal"),

- use of cryptic, uninformative labels for hypotheses ("H1", "H2", "H3", "H4"), and

- incomplete diagnostic message ("H4 confirmed").

The "after" design contains several manifestations of these design concepts for providing IS status "at a glance". They include:

- qualitative and quantitative description of the anomaly ("pump speed below nominal – current value = 430, nominal = 500"),

- distinction between anomaly, hypotheses, and diagnosis (through spatial and graphical organization),

- clear presentation of hypotheses,

- inclusion of all potential causes of the anomaly,

- indication of evidence for as well as against a diagnosis, and

- informative diagnostic message ("Diagnosis: Pump B1 Impeller Damage").

An approach from the research literature that addresses this problem is incorporated in the 'significance messages' display design (Woods, 1988b; Woods and Elias, 1988). This is an integrated display concept in which an analog graphic form is adaptively annotated with context-sensitive messages based on qualitative system state. The critical aspects of their design in terms of the informational properties of text messages are:

- **Icons to categorize each message.** These serve to cue the topic a message addresses. For the present application, these could be component based (RFMD, evap., etc.) or function based (heat load, subcooling, etc.)

- **Standard structure for each message.** The wording is designed to signal the exact state and related setpoint (since the focus was qualitative states relevant to a dynamic continuous variable). For the present application, components might include: (a) the state, event, or interesting behavior of the MP, (b) why the IS think this is interesting (this is usually based on a difference between actual and expected behavior), (c) the relationship between this anomalous state and the larger context of goals and activities (Woods, 1992).

Prior to this section, the emphasis had been on the macro level issues within a temporal information display. Now, however, the focus has shifted to a micro level and focused on the individual messages themselves. Despite this, the goal has remained virtually the same – to support the human operator's assessment and understanding of the anomalous situation through comprehensive, informative messages about the events in the MP and the activity of the IS. The alternatives discussed in this section are designed to support this goal by providing a standard structure to reduce visual search within a message.

## 4.8. Discussion

A fundamental aspect of fault management is that the human operator needs to know what the intelligent system is doing (at some level) and the state of the monitored process. He must track evolving situations laden with unanticipated events. As a result, he must build and maintain a coherent situation assessment in a changing environment where multiple factors are at work including one or more faults and operator and intelligent system intervention. As discussed previously, information processing in this domain is event driven, as the primary task is to determine, out of all the signal states and changes, which represent anomalies.

Overall, the problem with a typical message list is that it imposes cognitively effortful deliberative process of finding, collecting, and integrating individual messages in order to construct the meaningful relationships and patterns between events. This has direct implications for the design of systems to support human-intelligent system interaction. First, the intelligent system should help the operator see anomalies in the monitored process. Since anomalies are defined as mismatches, the fault management support system should help the operator see what specific mismatch is present (as indicated in Figure 15). Second, support should be provided for tracking the set of anomalies present in the monitored process and their temporal inter-relationships. As these examples have demonstrated, temporal information is often overlooked, yet is a central feature. Third, it is important for an intelligent system to assist the human operator untangle the interaction between the influences of faults and corrective responses. Providing an organizational structure such as discussed in this chapter is essential in this respect. Along these lines, one of the central points of the significance messages concept (Woods, 1988b; Woods and Elias, 1988) is that it uses:

"computer power for the *display of data in context* as an approach to building representation aids. The intelligence in the system is used, not to specify an answer for a

user. . ., but to create and manipulate the representation through which the domain problem solver sees the world. The AI based computer power is used to carry out overhead data processing and to manage the available data as a function of the context to help the domain problem solver focus on the relevant data and to avoid data overload." (Woods, 1988; p. 12 – italics in original).

The alternative approaches to the design of intelligent system output explored in this section are attempts to support the fault management tasks imposed on the operator through the representation provided by the computer medium. Chapter 6 will describe a specific design being developed for the TCS intelligent diagnostic system in an attempt to formally evaluate the applicability of the concepts presented in this chapter.

# 5. VISUALIZATION OF MONITORED PROCESS BEHAVIOR: DEVELOPMENT OF FUNCTION-BASED DISPLAYS

## 5.1. Introduction

While the previous chapter emphasized the flow of information from the IS to the human operator, the central issue in dynamic fault management, as discussed in Chapter 2, is the operator's ability to assess the behavior of the MP and be able to respond to anomalies. It is for this reason that the discussion thus far has focused on tracking the IS's activity *with reference to* events and anomalies in the MP. The present chapter will address more directly approaches to improve the operator's ability to visualize the behavior of the MP, one of the major weaknesses in the systems investigated in the case studies.

One motivating force for this work not yet addressed is the fact that as MPs become more complex, it also becomes increasingly difficult to present a complete representation of all of the sensors, meters, control settings, etc. in a single display. Thus the need arises for an overview display (also called summary, or status displays). For the purposes of the present discussion, an overview display will be defined as a display which attempts to present a representation of the state of the MP in one coherent view without explicitly including all of the measured or sensed parameters.

In a nuclear power plant, for example, an experienced operator can stand at the back of the room and gain enough information from the alarm annunciator panel to describe the status of the system (i.e., the current state, epoch, and activities of the system, etc.) Some of the features of this display system that facilitate state assessment are spatial dedication (a given alarm is always displayed in a given place), pattern recognition (a certain disturbance results in a unique "signature" of alarms), and information integration (many system parameters are represented by a single annunciator). If an overview display effectively summarizes system status, it will externalize pertinent information found within the display structure, thus allow an operator the opportunity to assess the status of the MP and to quickly see how the system is behaving. This can lessen an operator's mental workload when the computer is used to integrate information and show relationships that might normally be missed while an operator is focused on the details of a system.

It is also important to point out the several different uses of an overview display. Certainly the focus of this work is the function of monitoring system status for anomalies. In this context, operators would use an overview display as a primary indicator of health of the system. However, during the course of events, it may also be used as a starting point for navigating to other, more detailed displays. That is, an operator may see something going on and access additional displays to complement the information contained in the overview. Additionally, the overview display may need to be used to keep an eye on the process while the operator focuses on information in these

51

lower level displays (e.g., shrink it down and leave in the corner for use as an alarm indicator). These alternative uses, while certainly very important, are somewhat peripheral to the present discussion.

One of the major premises of this chapter is that the information requirements for an overview display and the approaches for its development are analogous to those for a function-based display (Rasmussen, 1986; Woods and Hollnagel, 1987). Therefore, the goal is to design a *functional overview* display for the TCS that will support the need for a summarization of system behavior as well as for providing an informative view of the MP. To this end, the following sections will discuss critical issues related to functional, temporal, and coordinative dimensions in terms of operator visualization of MP behavior (i.e., anomalies) and tracking IS activity in response to MP events. But first, though, typical approaches will be described to provide a framework for the subsequent sections. Weaknesses of these approaches will be discussed to support the issues presented, as well as design concepts and alternative representations to overcome these weaknesses. Given the context-dependent nature of this problem (i.e., an effective display cannot be designed void of domain semantics), examples from the TCS will be relied on primarily throughout this chapter.

## 5.2. Typical approaches

Virtually every interface to a monitored process (MP) investigated in the case studies contained a schematic diagram of the MP to depict the current state of the process being controlled. This type of display can be called a physical topology schematic because the organization of the graphical display is based on the physical topology of the MP – the subsystems, components, and their physical inter-connections. Active data about the state of the MP – parameter values or component states – are annotated to the schematic. Figure 20 presents a typical overview display from one of the systems investigated which includes a physical schematic to present information on the current state of the process. While not apparent from the figure, the dynamic portion of the display is entirely raw sensor data digitally displayed.

These types of physical schematics tend to be reproductions of paper-based schematic diagrams with certain modifications. It is important to be aware of the implications that these modifications have on an operator's ability to extract information on the status of the MP. One important difference (as mentioned above) is that the VDU-based physical schematic incorporates dynamic data; parameter values are placed physically next to, or on top of, the representations of the components or sensors associated with them. The schematic is effectively given a dual task – rather than simply provide a static view of the physical structure of the system, it is intended also to provide a dynamic picture of the state of the process.

The other important modification is imposed by the nature of the host medium; real estate on a VDU is precious and so many times the schematic cannot be presented in its entirety. In the TCS (as well as in other systems), the overview display has undergone a simplification of detail through filtering. That is, only a select subset (those deemed to be the most critical) of the sensor values are presented. A different approach would be to use a technique such as pan and zoom to move a viewport over the

entire, fully detailed schematic. In either case, the VDU schematic must be viewed in a different way from the way its paper counterpart can be viewed.

To illustrate this for the present context, Figure 21 depicts a simplified version of the paper-based physical schematic diagram of the TCS without indications of current sensor values. Note that this is different than the depiction in Chapter 3. The earlier figure was designed to be slightly more generic (i.e., flexibility in number of evaporators and condensers) than the present figure which is based on the blueprint schematics for the current version of the TCS ground-based test article. Figure 22 presents the top-level overview display for the TCS (entitled 'status-at-a-glance'). Despite the fact that the physical interconnections are not included in this display, the similarities in spatial arrangement is obvious. As mentioned above, only a subset of the sensor values are presented (24 out of more than 100), and in keeping with the example in Figure 20, raw sensor values are the primary form of dynamic information presented.
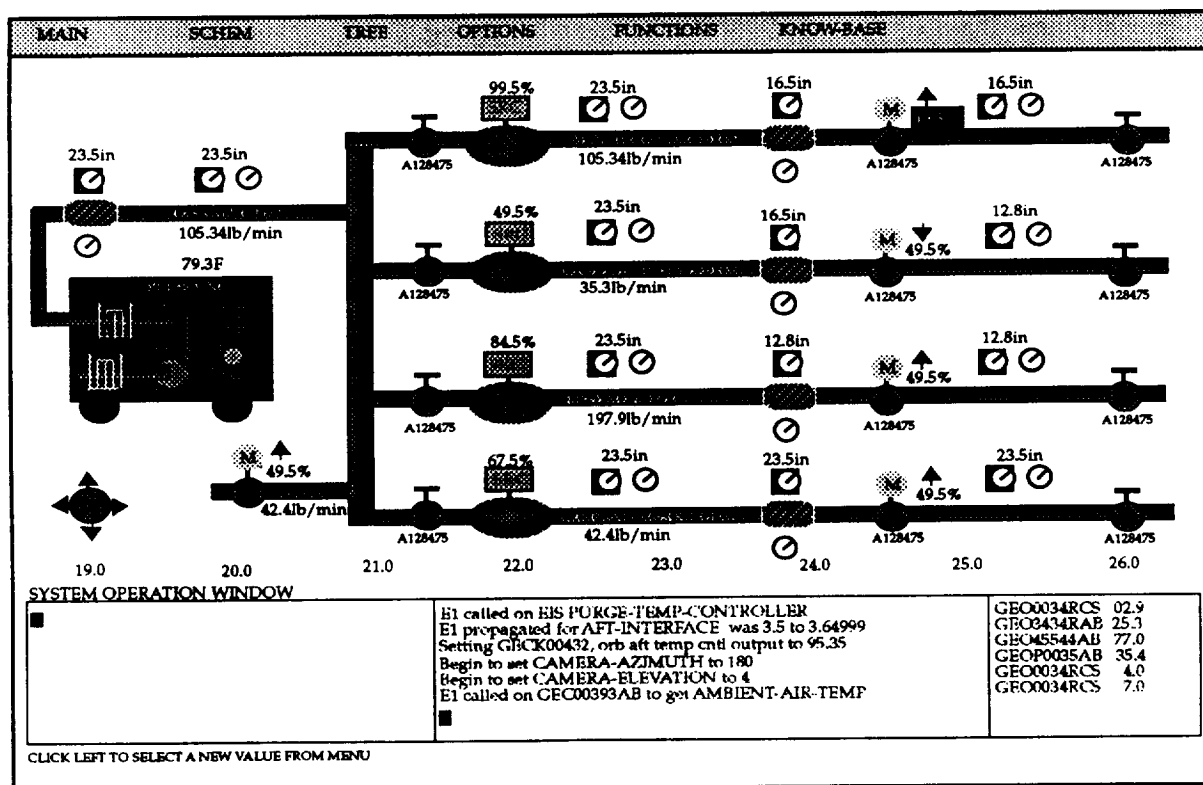


Figure 20. Typical overview display into the behavior of a monitored process, including physical schematic and message list.
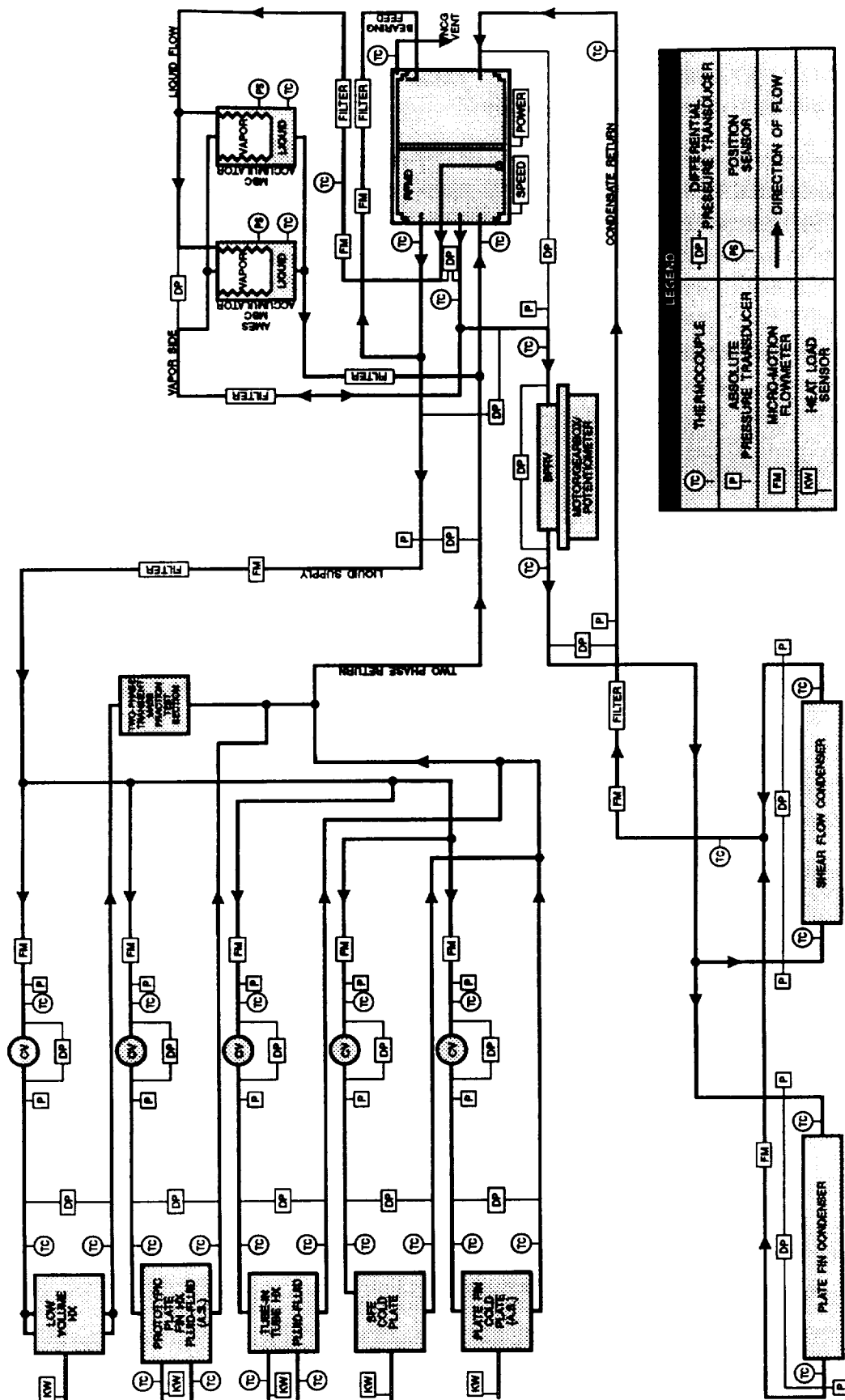
Figure 21. Physical schematic drawing of the thermal control system components and sensor locations.

## 5.3. Analysis of task demands vs. resources

While Chapter 2 discussed the cognitive demands of fault management, this chapter will focus on the specific information requirements, demands and difficulties associated with designing an overview display.

### 5.3.1. Informational properties of monitored process behavior

Some of the properties of a physical system that might need to be conveyed through a representational view include the following:

- current value of a given parameter,
- past values (values over time),
- future values (estimated by interpolation or calculated based on model of system functioning),
- limits, thresholds, targets, and goals (static as well as dynamic),
- relationships between/among parameters,
- qualitative states (e.g., on/off; enabled/disabled; normal/abnormal), and
- derived parameters (through abstraction, integration, transformation, collection) such as
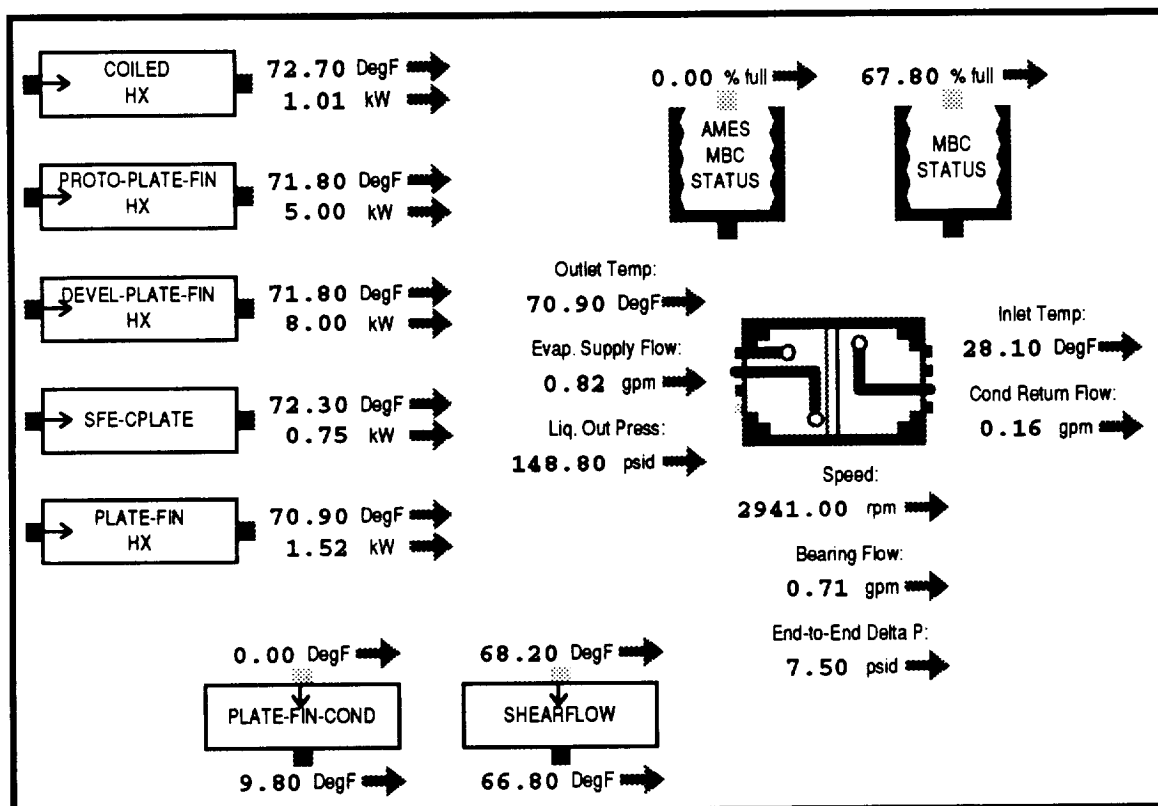


Figure 22. 'Status-at-a-glance' display for the thermal control system.

subcooling margin or compensated level (Woods and Roth, 1988).

With one of the primary goals being to improve the operator's ability to detect deviations from normal and isolate anomalous behavior.

### 5.3.2. Task demands/bottlenecks

Problems in communicating the information outlined above include:

- complex systems with many sensors,
- limited real-estate on which to display information,
- need to minimize interface burdens (i.e., to create a "transparent" interface),
- difficult task of analyzing system functioning to determine critical information to display, and
- problem of highlighting anomalous behavior in the context of the normal ebb and flow of events.

### 5.3.3. Design basis

The problem, then, is how to capture the above-mentioned informational properties into a display design that works around the problems and limitations described. However, at a deeper level, in order to design an effective overview display of the MP it is imperative to define the information that operators need to perform their tasks (i.e., what are the information extraction goals for this display?). A physical schematic of the monitored process is useful if the operator needs to know about the different physical parts of the system and their interconnections. For example, knowing where a sensor is located relative to other sensors/components may be important in extracting the significance of its current reading or recent behavior under some conditions. However, physical schematics are often used when the information transfer goal is to show the state of the monitored process – is it working correctly? is it achieving its goal? – typical goals of an overview display.

## 5.4. Beyond digital data display

### 5.4.1. Problem description

One of the primary features of the examples in Figures 20 and 22 is the abundance of digitally-displayed data. In fact, with respect to the TCS (except for one exception to be discussed in the next section) this is the *only* way information is conveyed. The advantages of this approach include:

- economical in terms of real-estate,
- complies with a physical-oriented schematic (data is placed next to the component's icon), and
- economical in terms of interface development (easy to code).

On the other hand, much has been written in the past (e.g., Van Cott and Kinkade, 1972; McCormick and Sanders, 1987; Boff and Lincoln, 1988) about the limitations of digital data display. These include:

- difficulty in assessing qualitative state (approximate value, trend, rate and direction of change, deviation from a desired value)

- difficulty in establishing a parameters context (how close to target or limit) without undue memory burdens,

- lack of integration and association of related data, and

- difficulty in discriminating significant from non-significant changes (i.e., highlighting anomalies and state changes).

## 5.4.2. Examples

In the system depicted in Figure 20, a physical schematic served as the primary means for displaying information and navigating to other menus and displays. The schematic shows digital parameter values which are dynamically updated. Because it was expected that operators would have trouble detecting changes in the monitored process when inspecting the schematic, another smaller, scrollable window was placed in the lower, right-hand corner of the screen to show the most recent changes in parameter values as a message list. Each time a parameter changed, its ID number and new value were added to the bottom of the list. To infer direction and rate of change, the most recent posting must be compared with the next-most-recent of the same parameter.

This second window attempts to deal with some of the limitations of digital data display (in particular the problem of calling the operator's attention to parameter changes). While it may be easier to detect changes in the MP through the smaller window in a situation of low frequency changes, there are several reasons why this is a poor strategy for presenting information in the dynamic, complex domain of fault management. First of all, data is being repeated within the same viewport. Instead, it should only appear once, effectively displayed. Having the data displayed in two locations forces the operator to switch attention back and forth among views in order to integrate the information presented in them. This "dissociation of data" is inefficient and effortful. Second, the designers have replaced one effortful strategy (carefully monitoring the schematic display for changes) with another (relating the two sources of information; finding the relevant updates from the message list and calculating deviations). Note that without timestamps, rate of change information for the component values is actually not available – even in the small window. Finally, given any amount of dynamism in the MP, it can be assumed that relevant entries in the message list will be difficult to extract (similar to the problems with this type of format discussed in Chapter 4).

The 'status-at-a-glance' display in the TCS used a different approach to deal with the limitations of digital data display. Next to each of the sensor values are arrows designed to depict trend information. These arrows are driven by the slope of the least-squares regression line for the most recent 20 seconds of sensor data (since data is updated every five seconds, four data points are used in this equation). Based on this slope information, the arrows can take on three states – flat (within a tolerance around zero), up (above tolerance), or down (below tolerance).

While this approach, like the previous example, recognizes the need for creating more informative displays, there are several problems with the resulting design. First, it only indicates direction of change and provides no indication about rate of change. A relatively small increase appears the same as a large, rapid increase. This tends to over-emphasize minor changes and under-estimate large

ones. In fact, one of the comments on this display was the "startling" nature of the changes in the display. Given that all sensor movement is depicted the same, the only way for an operator to distinguish between significant and insignificant behavior is to focus on the digitally displayed sensor values. It should be noted that more fine-grained movements could overcome this limitation. Second, this approach fails to capture deviations from nominal (high or low), which can be deceiving. For example, a parameter that is "high and decreasing" is recovering – behavior quite different from "low and decreasing". That is, given the same behavior of the graphic form in different contexts (high vs. low), the operator is forced to interpret the digital value and direction of change to infer if normal, expected, or anomalous. Also, given the spatial arrangement which promotes thinking about physical connections between components, there is the possibility of confusion over the arrows as direction of flow indicators (a common element in physical schematic displays). This is especially important for the TCS since the flow to the condensers can actually go in either direction.

At a higher level, given the dynamism of fault management in general (as discussed in the first section) and of the TCS specifically, the "normal" state of the 'status-at-a-glance' display will be to have continual changes in the system depicted by continual changes in the trend arrows. This is very important, even with a least-squares approach to data smoothing. If many things are changing normally as background (nominal) behavior, then detecting anomalous movement becomes a much more difficult task.

### 5.4.3. Design concept(s)

(1) Recognize limitations of digital data display for dynamic environments.
(2) Construct a design basis to uncover limits, thresholds, etc. which need to be conveyed through analog forms.
(3) Recognize functional as well as physical relationships and support both in the display design.

### 5.4.4. Alternative representations

In terms of alternative approaches, they can be divided into two groups: "strong" and "weak". The weak approaches involves adding coding techniques to the currently available digital data. Examples include color coding for limit crossings and graphical augmentations.

1. **Color coding.** The approach incorporated in the example in Figure 20 is the use of coding techniques in addition to the currently available digital data. While one approach is the more traditional use of yellow to indicate cautionary conditions and red to indicate warnings (limit crossings), this case uses a somewhat different coding scheme. Red is used to indicate deviation from a model-based prediction, purple is used to indicate that the IS has "explained" the discrepancy (e.g., isolated a faulty component or sensor), and other, non-pertinent colors are used. See Woods, et al., (1991) for a more detailed description of the implications of this type of coding scheme. Subsequent sections will provide more details of the use of the IS to provide context in which to interpret the behavior of the MP.

**2. Graphical augmentation.** Another approach is to augment the digital values with graphic forms in an attempt to provide additional information about the behavior of the particular parameter. These include dynamic icons (to depict component state such as "on" and "off", "flow" or "no-flow" as in flow path coding, or "open" and "closed" as in electrical switches), continuous trend arrows (to depict direction and rate of change), and compact analog forms (to give an estimate of magnitude or state). The key to this type of approach is to start to use the dynamic nature of the computer medium to perceptually emphasize events and MP behavior.

A "strong" approach involves determining the system properties of interest and establishing the mapping between these properties and the structure and behavior of the interface (Rasmussen, 1986; Woods and Hollnagel, 1987; Woods and Roth, 1988b). This approach will be an integral part of subsequent sections, so will not be elaborated on here.

## 5.5. Emphasize relationships between parameters

### 5.5.1. Problem description

As mentioned in the previous section, more important than conveying the absolute value of a given parameter, an effective display design conveys information about relationships (Woods, in press). This includes relationships between actual and expected behavior, between related parameters, and between events and behavior. One of the key issues is that of comparison against a reference. That is, data becomes informative when it is placed in context. Some of the questions a TCS operator might be asking when in need of information about relationships are:

- Which evaporator has the greatest heat load?
- What's the exit quality on that evaporator?
- Temperature return from that evaporator is high – is it getting too much heat load?
- Current system temperature is 72°F – is that where it should be?
- Is flow rate sufficient for cavitation?
- What is the subcooling margin?

### 5.5.2. Design concepts(s)

(4) A cognitive task analysis must be performed to identify important data relationships to be emphasized in the overview display.

### 5.5.3. Alternative representations

**1. Emphasize constraints and relationships.** An interesting example of capturing relationships between parameters is found in Vicente and Rasmussen (1990). Figures 23 and 24 present a physical and functional overview display of a thermal-hydraulic control system. The goal of the system is to deliver water from each of the reservoirs at a desired flow rate and temperature. This requires controlling input flow to the reservoirs to maintain enough water to satisfy the output flow demand and to control heating of the water within the reservoirs to satisfy the output temperature demand.

One of the interesting aspects of this system is the constraining relationships within the system. First, each feedwater system serves both reservoirs. So, at the VA and VB valves a change in valve position will impact flow rate (and thus level) to both reservoirs. This may have the desired effect for one but the unwanted effect for the other. Second, within a reservoir there is a unidimensional constraint between volume and temperature control. That is, if one adjusts temperature to achieve the desired setpoint and then adjusts flow, the change in volume will require another change in temperature control. Thus, it is important to convey this relationship through the interface, as they have done in the functional display.

**2. Include background coding to emphasize physical and functional interconnections.** First, it must be decided what aspect of the system is to be emphasized in a particular display. If the purpose is to convey physical interconnections between components, then the details of the system need to be included. For example, several of the subjects in the present work confused the trend arrows (in their nominal position) with direction of flow (a fairly common element in physical schematic displays). Also, there was some confusion as to exactly which sensor was being displayed for "outlet temp"
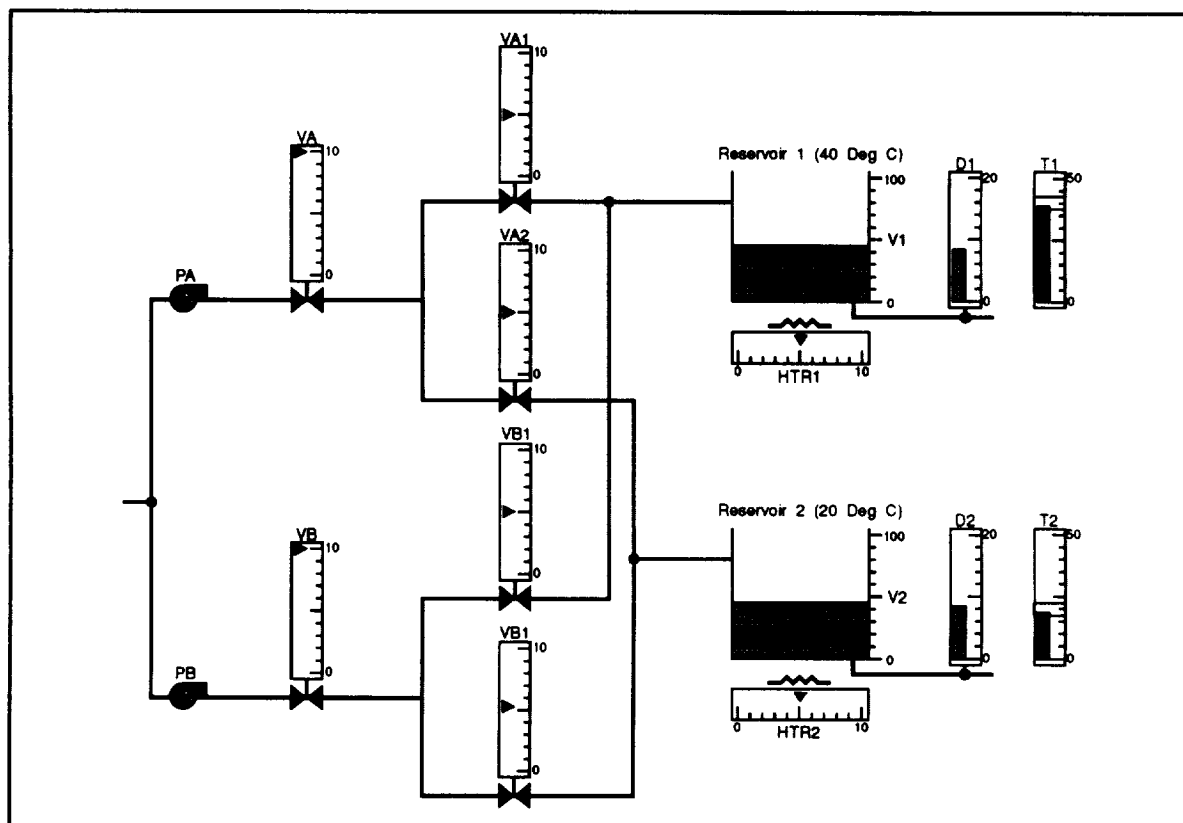


Figure 23. Physical interface for the thermal-hydraulic control system investigated by Vicente and Rasmussen (1990).

(i.e., RFMD outlet or evaporator outlet). This is an inherent problem in a filtering approach to develop overview displays. Thus, if it is important to specify which particular sensor is being displayed, then showing the physical interconnections can serve to provide the appropriate context.

**3. Utilize computed parameters for establishing context.** For the TCS (as well as for several of the other systems investigated), the IS developers have built a model-based system to generate expected values for the critical parameters. This model-based system was developed as an approach to overcome the complexity of the MP which goes beyond fixed critical values. While these parameters were used by the IS (for diagnostic purposes), they were not used to enhance the representation of the MP for the human operator. However, this approach can provide an extremely useful context against which to compare current values. In addition, there are generally setpoints and goals that the system is attempting to achieve (e.g., the TCS can be configured to operate at 70°F or 35°F).
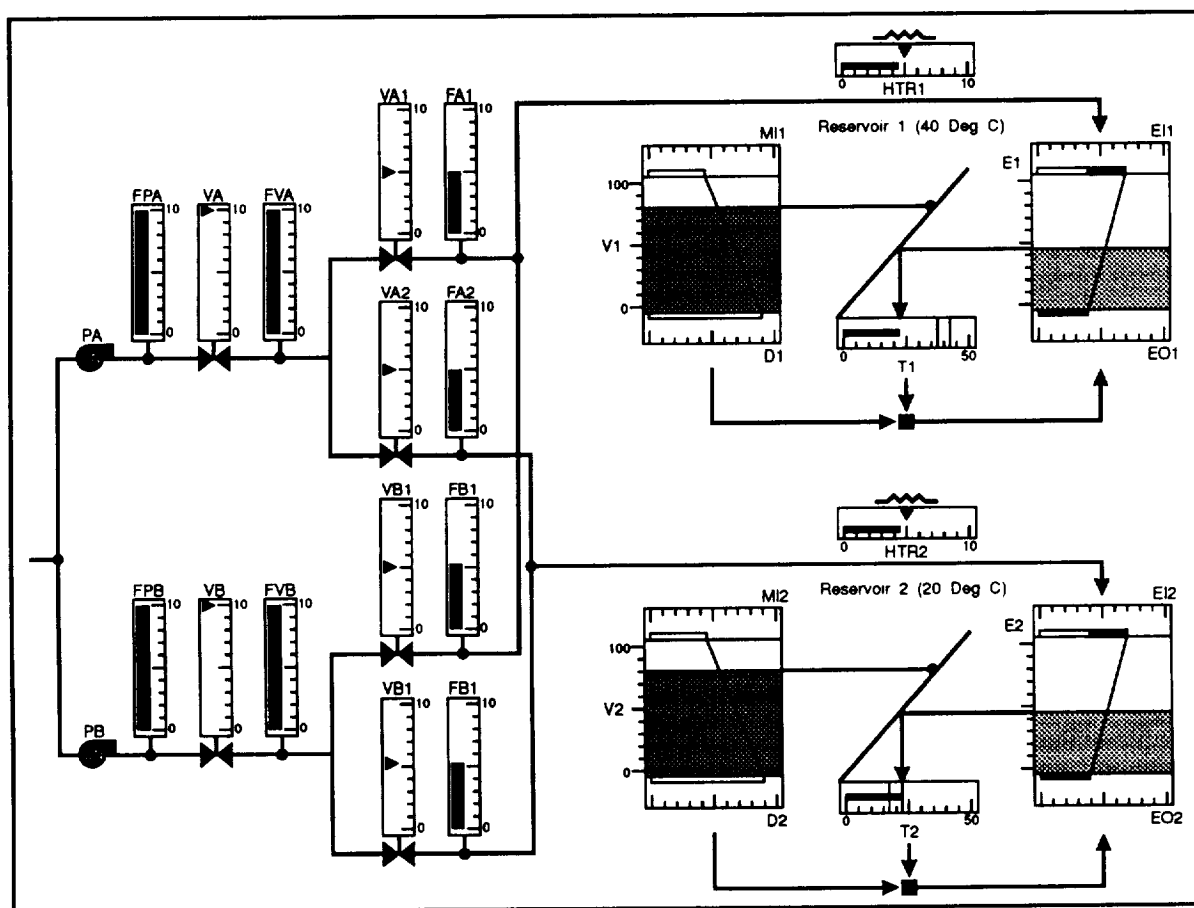


Figure 24. Functional interface for the thermal-hydraulic control system investigated by Vicente and Rasmussen (1990).

It is important to note the difference between these two types of referents. A real-time computed parameter is dynamic and based on current system conditions. This is not equivalent to static nominal values which must be prespecified. A computed parameter may fluctuate considerably depending on system behavior (e.g., current conditions, epochs in task evolution, and configurations). While a particular system setpoint or goal can also vary, these are usually commanded or mode-dependent. In fact, Wickens (1992) claims that for complex systems (such as TCS) static, prespecified limits are not feasible due to the inherent system variability. There are simply too many possible modes and configurations to consider.

Figure 25 presents three examples of emphasizing relationships between parameters within the TCS. In panel (a) evaporator outlet temperature is the focus, panel (b) – accumulator level, panel (c) – system setpoint temperature. For evaporator outlet temperature, current values are plotted against the expected value based on the IS's model-based calculations. To accommodate different hardware configurations, only the total, maximum, and minimum evaporators are included. The maximum and minimum evaporators are indicated by labels below the graphs. Anomalies such as evaporator blockage and overheating would be manifest in an increasing outlet temperature and a deviation from the expected value. The example in the figure demonstrates (from left to right) an increase in individual evaporator outlet temperature that eventually impacts the aggregate temperature.

For accumulator level, current levels are plotted against predicted level, only this time these parameters are plotted against a fixed scale (0 to 100% full) since the predicted value changes quite frequently. Also, a history plot is included to emphasize differences over time. The predicted level provides an indication of future conditions (this will be discussed in more detail in the next section). For example, the middle panel indicates a situation where level in one of the accumulators is high but the predicted value is decreasing, indicating recovery. An increasing differential between actual and expected (as in the right panel) indicates a slow leak in the system.

For system setpoint temperature, three indications of system status are included. They are (1) "measured" – current actual sensor reading, (2) "predicted" – based on the position of the BPRV (valve position transformed into temperature), and (3) "calculated" – based on the current system pressure (pressure transformed into saturation temperature). Note that these are all plotted against the fixed setpoint temperature of 70°F (to show deviations from the "target" value – this is constant unless the system is reconfigured to the lower setpoint). In this context, the model-based expected value is not presented because (1) the target is always constant and (2) the emphasis is on comparing the three assessments of system setpoint temperature to convey conditions within the TCS. The middle and right panel of this portion of the figure depict mismatches between the measured and predicted values, indicating a disparity between current conditions and BPRV setting.

(a.)

**Evaporator Temperature**

| Max | Total | Min |
|---|---|---|
| 73.70 | 70.30 | 68.30 |
| 84 | 84 | |

70 · 70

56 · 56

**TUBE-IN-TUBE HX** · **PROTO-PLATE FIN HX**

**Evaporator Temperature**

| Max | Total | Min |
|---|---|---|
| 76.40 | 70.80 | 69.30 |
| 84 | 84 | |

70 · 70

56 · 56

**LOW VOL HX** · **PROTO-PLATE FIN HX**

**Evaporator Temperature**

| Max | Total | Min |
|---|---|---|
| 76.40 | 75.60 | 71.50 |
| 84 | 84 | |

70 · 70

56 · 56

**LOW VOL HX** · **PLATE FIN COLD PLATE**

(b.)



(c.)

**Setpoint / System Temperature**

| Meas. | Pred. | Calc. |
|---|---|---|
| 70.10 | 72.30 | 70.00 |
| 84 | 84 | |

70 · 70

56 · 56

**Setpoint / System Temperature**

| Meas. | Pred. | Calc. |
|---|---|---|
| 70.10 | 75.40 | 70.00 |
| 84 | 84 | |

70 · 70

56 · 56

**Setpoint / System Temperature**

| Meas. | Pred. | Calc. |
|---|---|---|
| 76.40 | 71.30 | 70.00 |
| 84 | 84 | |

70 · 70

56 · 56

© 1992, Potter and Woods

Figure 25. (a) evaporator outlet temperature, (b) accumulator level, and (c) system setpoint temperature displays. See text for details.

**4. Highlight *functional* constraints and relationships between parameters.** In addition to physical constraints (such as the relationship between heat load and evaporator capacity) where there is a direct relationship between system parameters (i.e., excessive heatload will overload that particular evaporator for a given flow rate), it is also important to include functional constraints – that is, more indirect relationships. For example, the BPRV adjusts flow to the condensers to accommodate the heat load imposed on the system. There is a limit, though, on the condensers capacity to dissipate heat. Depending on conditions, this may be higher or lower than the aggregate evaporator heat load capacity. This is the type of information that may best be conveyed by the IS (through the message list) or through an annotated schematic display (Johns, 1990).

One implementation of this approach is the significance messages concept (Woods, 1988b; Woods and Elias, 1988) briefly mentioned in the previous chapter. The central part of the display is an adaptive analog graphic of the primary system variable (demonstrated for "pressure" in a pressurized water nuclear reactor). Augmented to this graphic are messages about system behavior linked to the critical value for the particular message. This provides an integration of information from all system components and presents them in terms of their functional relationships. For example, some of the messages are related to events that will occur if level continues in the current direction, forming adaptive, functional context in which to interpret system behavior in addition to insights into functioning of other system components.

## 5.6. Convey system status "at a glance"

### 5.6.1. Problem description

The point of an overview or summary display is to present relevant information in a concise, recognizable form. The relevant information must be represented in a way that can be processed at a glance. (One indication of a concise overview display is that it continues to convey information even if reduced to a smaller size.) Summaries in which information is solely conveyed through the digital display of data are not concise because they require manipulations and comparisons to establish the appropriate context to be interpreted.

Much research has been conducted on the design of object, or configural displays for the presentation of high-level system functioning (Bennett and Flach, 1992; Bennett, Toms, and Woods, 1993). Based on this previous work, several critical aspects of display design have been identified. These include: semantic mapping, emergent features, and perceptual segmentation. The following sections will outline these critical aspects of display design related to mentally economical processing of system status information. One aspect of this design effort that has not been addressed to nearly the same extent is the problem of how to transform an operators view of the state of the MP from raw sensor values (which, even displayed digitally cannot all fit on one CRT) to integrated, informative graphics. This will be discussed in the next section.

In order to focus this problem with respect to the TCS, it should be helpful to consider the types of questions that would be of primary interest at the overview display level. These include:

- is the system maintaining setpoint temperature?
- are all the heat loads to the evaporators within limits?
- is there any evidence of excessive temperatures in the evaporator outlet?
- is inventory (accumulator level) being maintained?

To answer these questions through information contained in the 'status-at-a-glance' display (as presented in Figure 22) would require (respectively):

- comparing the "outlet temp." value (temperature of the liquid supply to the evaporators) to the setpoint temperature (70° or 35°). However, it was identified that this parameter is not actually the best indicator of system temperature. Vapor temp. (as discussed in the previous section and illustrated in panel (c) of Figure 25) provides a more accurate indication of system behavior.

- comparing the digital heat load display (to the right of each evaporator icon) to the pre-defined maximum heat load capacity for each evaporator (must be recalled from memory or referred to in documentation).

- comparing the evaporator outlet temperatures (to the right of each evaporator icon, above the heat load display) with the setpoint temperature (70 or 35). However, there can be some fluctuation in the "nominal" evaporator outlet temperature depending on current conditions within the system.

- monitoring accumulator levels and detecting low values (static limits are 20 and 80% full). However, there is considerable fluctuation in these levels so that a decreasing value does not indicate loss of inventory.

## 5.6.2. Design concepts(s)

(5) A cognitive task analysis must be performed to identify the critical semantics of the domain to be captured in the behavior of the representation.

(6) Design a coding system that takes into account the relative impact across a set a set of coding attributes. Objects, forms, and groups have attributes that jointly produce their perceived relative impact.

## 5.6.3. Alternative representations

**1. Establish the mapping from domain semantics into syntax of the visual form.** This is one of the key elements of representation design (Woods, in press) and a central issue in the next chapter which discusses the display design for TCS. The critical question is how data on the state and behavior of the domain is mapped into the syntax and dynamics of visual forms in order to produce information transfer to the agent using the representation given some task and goal context. What matters, then, is not how the computer graphics look but how the graphics represent (i.e., not the "object-ness" per se, but the relationship between information demands of the domain and features of the display design). What needs to be emphasized based on the types of questions outlined above should in fact be emphasized in the interface. The purpose of thinking about the types of questions to be addressed at this level is to emphasize the fact that the questions of interest are different than the type of information able to be extracted from typical schematic displays.

For example, the critical domain semantics from Figure 25 are (a) are any of the evaporators experiencing an increase in temperature (rather than the precise outlet temperature of the individual evaporators), (b) are the accumulator levels at their expected level (which varies dependent on current conditions of the TCS), (c) is the system maintaining setpoint temperature (which is defined at 70°F or 35°F). Notice that in each of these examples the important piece of information is the relationship between variables rather than the precise parameter value. Digital data display forces the operator to perform data manipulations and comparisons in order to construct these relationships.

**2. Capitalize on emergent properties of the display.** Emergent properties refers to perceptual aspects of the display that inter-relate to produce additional, "higher-order" properties. Bennett, Toms, and Woods (1993) define emergent features as "highly salient visual properties that arise from the interaction between lower-level graphical elements." As in the previous section, it is critical that the emergent features of the display correspond to the information requirements of the domain. In their design, four critical process variables are mapped onto a single geometric object (a rectangle). While critical relationships are directly mapped onto the height and width of the rectangle, additional emergent properties include area and shape of the rectangle, the location, direction and rate of movement of the rectangle within the display grid.

One example of an object display that takes advantage of emergent properties of the display is the safety parameter display system developed by Woods, Wise, and Hanes (1981; also Woods, OBrien and Hanes, 1987), depicted in Figure 26. Critical system parameters (more than 100 in total) are integrated and normalized into the axes of a polygon. Normal/abnormal distinction is facilitated by the "regularity" of the octagon. In addition, a variety of different anomalous states can be distinguished by specific contortions of the octagon, supporting fault diagnosis in addition to fault detection. Experimental research has supported the use of this type of approach to collect and integrate parameters in a process control environment (Jones, Wickens, and Deutch, 1990).

**3. Perceptual segmentation.** In addition, it is important to design the perceptual characteristics of the display to emphasize the critical aspects. It seems obvious to say that what is important should stand out; the operator should not have to expend effort in finding out needed information. In general, change can be said to be important and should be conspicuous. Yet as the examples in Figures 20, and 22 demonstrate, the case study discovered schematics and other display forms where the most perceptually salient features were static, non-pertinent elements such as the representation of the physical system, the name of the system or of the organization. In general, the physical schematics failed to help the operator see the patterns of events and quickly size up the dynamical state of the monitored process.
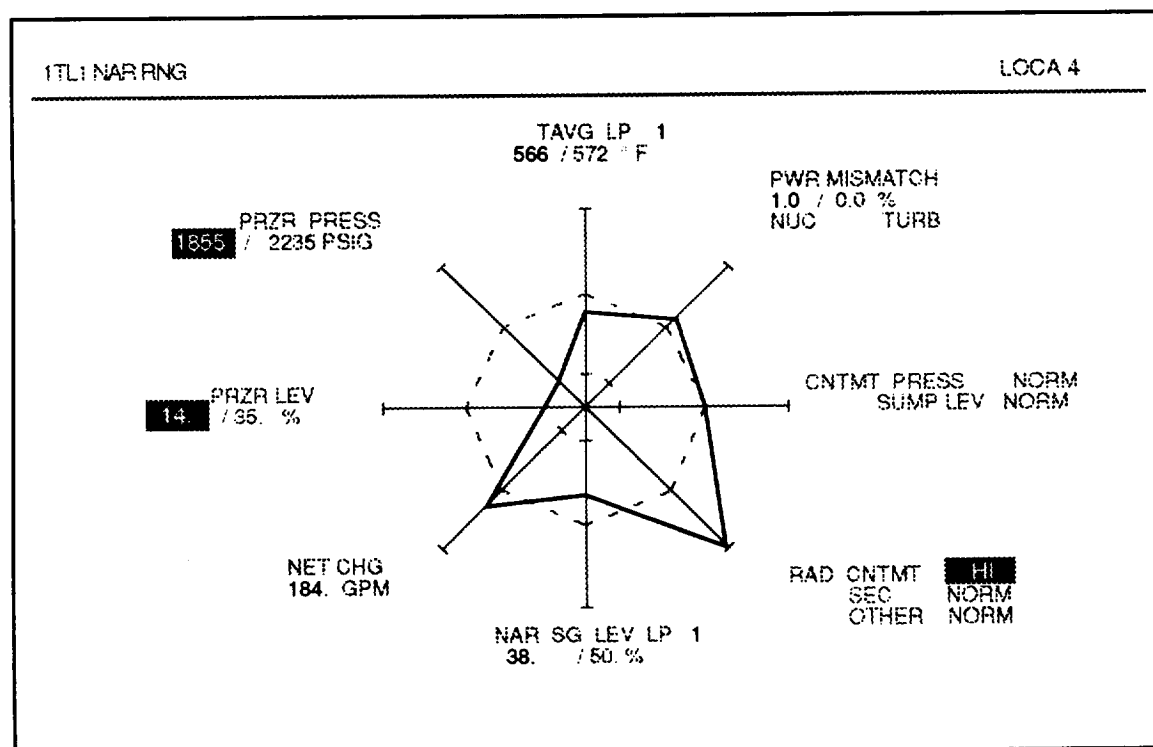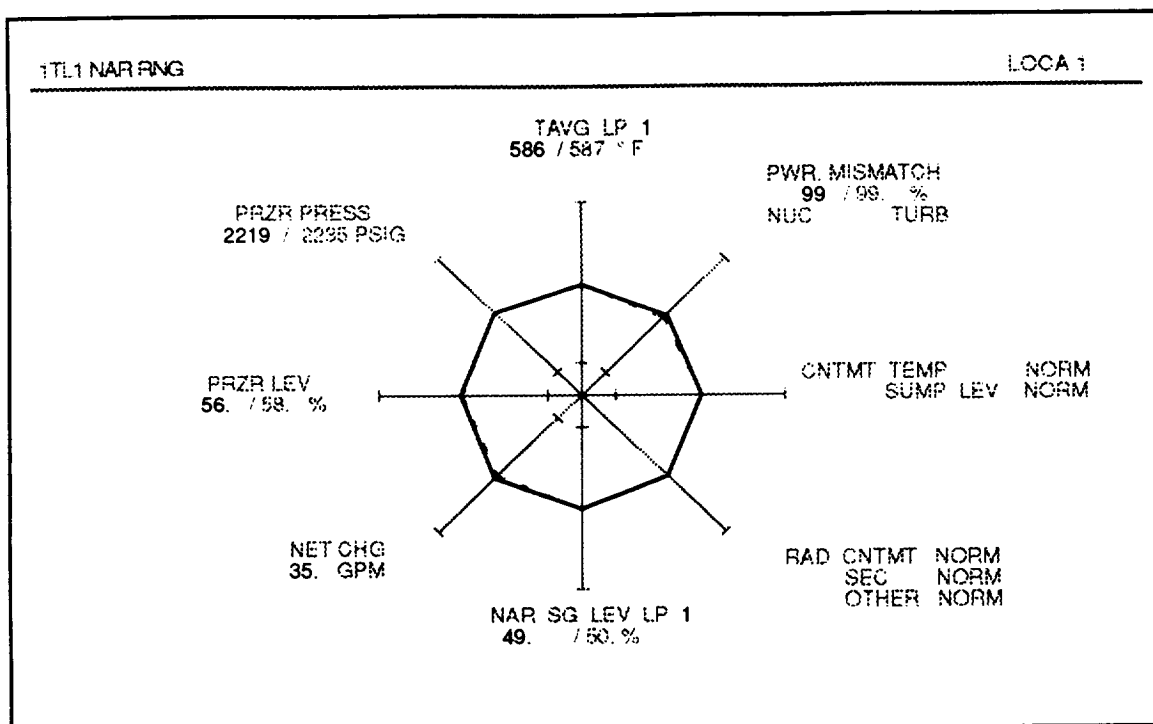
Figure 26. Two examples from the Safety Parameter Display System (Woods, Wise, and Hanes, 1981).

The perceptual saliency of the various objects should correspond to their importance within the overview display. To go further, though, one needs to think about the saliency of events and behavior within the system. For example, the use of trend arrows in the 'status-at-a-glance' display imposes consistent coding to all temporal changes. That is, every increase in a given parameter is conveyed in the same manner, no matter how extreme or whether the parameter is deteriorating or recovering.

Typically digital data display is enhanced with color coding to highlight anomalous values. It is important, though, to consider the attributes of the entire set of objects within the display when implementing such an approach. For example, a pure red object is less intense, or bright, than a white object, reducing its salience. However, if there is only one red object in the display, it is salient due to the lack of competing hues. Thus, a digital value coded red within a display of multi-colored icons may not be as salient as the designer intended. See Woods, Johannesen, and Potter (1992) for more on the use of color in HCI design.

## 5.7. Functional model of system behavior as a design basis

### 5.7.1. Problem description

Wickens (1992) points out that effective process control requires three important components:

- a clear specification and understanding of the future goals of production – a *command input*,
- an accurate *mental representation* of the current state of the process, and
- an accurate *mental model* of the dynamics of the process.

This section will focus on the last of these components, supporting the operators internal model of the system dynamics. To start, it is important to define what is meant by a "functional model of system behavior." Vicente and Rasmussen (1990) define functional structure of a system as "the set of constraints on achieving the systems objectives." They go on to describe several different types of constraints:

- **global** – purposes for which the system was developed,
- **holonomic** – laws that describe the functioning of the system (i.e., laws of thermodynamics),
- **nonholonomic** – boundary conditions set up by the system design.

Mitchell and Saisi (1987) define a functional model (specifically, their operator function model) as a "formal structure that represents how an operator decomposes a complex system into simpler parts and coordinates control actions and system configurations so that acceptable overall system performance is achieved."

It is apparent that the use of "functional model" differs between Rasmussen and Mitchell. The important distinction is that Rasmussens approach is toward a structural model of the physical system while Mitchell focuses on a behavior model of the operator interacting with the system. This is addressed by Mitchell and Saisi:

> "Whereas Rasmussen primarily addresses decisionmaking in novel situations, i.e., rare events or singular situations caused by major disturbances, technical faults, human error,

or some combination, the operator function model represents decisionmaking in the normal operator functions of monitoring, fine tuning, as well as predictable fault detection, diagnosis, and compensation." (Mitchell and Saisi, 1987; p. 574)

As is certainly evident from the discussion to this point, this work has adopted the orientation of Rasmussen and is focusing on a model of the MP in order to convey the critical constraints to the operator. More formally, the use of the term functional model will refer to:

- system goals (that which is to be achieved, maintained, delivered, etc.),
- higher-order functional variables (as opposed to unprocessed sensor values),
- functional dynamics of system components (input-output control dynamics)

The basic problem, then, is how to represent functional properties through the user interface. Digital display of data in and of itself does not preclude the inclusion of functional properties. However, physical schematics consisting of solely raw sensor values are in fact void of any computed or processed higher-level information.

As an example, consider the system depicted in Figure 20. One of the primary goals of this system is to deliver a certain volume and temperature of gas to the four systems. However, these goals are not presented in the overview display at all. Instead, they must be maintained by the operator and compared to the current values of the sensed parameters.

### 5.7.2. Design concept(s)

(7) Several approaches exist – goal/means decomposition, operator function modeling – to construct a model of system behavior. This type of cognitive task analysis must be performed to capture critical functional relationships.

(8) At the overview level of display design, functional relationships and constraints must be identified and integrated into the interface design.

### 5.7.3. Alternative representations

1. **Identify and convey system dynamics.** The overview display must include information about the dynamics of the system. If an operator is assessing system status, he or she must be able to recognize patterns of change within that system. In addition to information about the current behaviors and states of the system, information about what has happened recently, and what kinds of trends may be developing often contributes to the overall assessment of the system status. The overview display should represent the dynamics of the system during both normal and abnormal system states. For example, if abnormal system states often result in a cascade of disturbances, the overview display should provide the necessary information to support an operator who is diagnosing the system. In some instances, the display could even remind the operator of potential sub-problems that usually occur when a more general problem like the malfunction of a specific system occurs.

For example, the system investigated by Roth and Woods (1988; also Woods and Roth, 1988b; Bennett, 1991) involves manual control of feedwater flow in the startup of a nuclear power plant, a

task that is analogous to the control of a parameter that has a minimum of third order control dynamics and considerable time lag. Much work went into the development of a predictor display to assist the human operator in this very difficult task. The critical issue is that their analysis identified critical system functional relationships (most notably compensated level) that can greatly improve an operators internal representation of system dynamics and thus system performance.

As mentioned earlier in this chapter (and indicated in Figure 25), a predictive indicator of accumulator level was identified as an important functional relationship within the TCS since system time lags (i.e., time to pump liquid from RFMD to accumulators) can impact the relationship between input (change in heat load) and output (liquid level in the accumulators). Together with a historical strip chart, this approach provides an indication of where the level has been and where it is heading.

**2. Include abstracted (not simplified) information.** To broaden the view of the system, information in the overview display should be abstracted to a higher level of information than that of raw sensor values and other low-level details about the system. It is important to note that abstracted information is not simply a lack of detail, but rather an informative integration of details. It involves collecting information from various areas of the system as well as comparing relevant system information. To do this, the designer may need to transform lower level data into parameters that integrate this data in a way that makes sense to an operator in his task context. Examples of abstracted information include answers to questions like: a) What mode is the system working in? b) Is the system functioning normally, or is there a malfunction in one of the subsystems? c) What activities are taking place at this time?

Three examples exist for the TCS. First refers to the performance of the cavitating venturis to deliver adequate rate of flow to the evaporators. As mentioned in Chapter 3, there is a relationship between input and output pressures that determines the coefficient of flow. Based on laws of fluid mechanics and through system testing it has been determined that a flow coefficient of $\leq$ .85 is required for constant flow rate. Second refers to the performance of the condensers. In the scenarios at the end of Chapter 3 it was discussed that the TCS requires a subcooling margin of 5 - 10°F for adequate performance. Subcooling is a concept that has been mentioned elsewhere as a critical parameter in thermodynamic systems (Goodstein and Rasmussen, 1988). The third example relates to heat acquisition. The critical performance parameter is the exit quality (percentage of ammonia vaporized) by the evaporators. This parameter, as the next chapter will discuss further, is a function of heat load and flow rate to the evaporators and provides a means to assess heat acquisition across evaporators with differing capacities.

## 5.8. Discussion

As each of the systems investigated in the case studies were attempting to build an overview display, the importance of providing system status "at a glance" as well as the inherent limitations in current

approaches has certainly been recognized by the system development community.[1]  Overall, the problem with typical physical schematic displays is that, at one level, they do not utilize the capabilities of the available graphical computer medium.  At another level, they tend to be focused on raw, unprocessed sensor values, leaving the comparisons and manipulations to the experienced human operator.  At a deeper level, though, they fail to make intelligent use of the available graphics through a disciplined approach to establish the mapping between domain semantics and syntax of the visual form.  The primary theme of this work is enhancing the operators ability to determine, within the normal ebb and flow of the state of the MP (and the associated parameter changes), which changes represent anomalies and build a coherent assessment of the state of the MP.

To this end, this chapter has described critical issues in the development of an function-based display as a means to enhance a human operators ability to assess the status of the MP.  As mentioned in the introduction and made apparent in the discussion of this chapter, this work is concerned with functional modeling as a tool or approach to information design for the human operator.  This is not the same as the functional reasoning work in which functional models are used to build more robust ISs (K. Abbott, 1990).  However, as the next chapter will show in more detail, the two approaches certainly are complementary.  Several parameters computed by the model based portion of the TCS IS proved to be very useful in emphasizing relationships between parameters and depicting system dynamics in the user interface.  In this manner, a function-based display can be designed to utilize the ISs power to help the human operator visualize the behavior of the MP, such as changes in the pattern of disturbances over time.  By integrating the results of the ISs computations (e.g., model based expectations) into the display of the state of the MP, the function based display helps realize the concept of a shared frame of reference for the support of joint human-machine cognitive systems (Woods and Roth, 1988b).

Together with Chapter 4, the framework has been laid for the specific integrated design for the TCS, which is the focus of the next chapter.

---

[1] After a discussion between the author and one of the system development groups on issues related to the design of overview displays (and their realization of what is needed to design a true 'status-at-a-glance' display), one of the team members said "Well, what about calling our overview display 'status-at-a-slightly-longer-glance'?"

# 6. REPRESENTATION DESIGN

## 6.1. Introduction

Given the information contained in the previous chapters, this chapter will discuss the development of the specific design for the TCS. This will consist of two primary sections. First, the methodology employed will be discussed; second, the resultant design will be presented. The focus of this chapter will be on the representation form (as discussed in the previous chapter) and the informational aspects of the design. In several instances, different choices could have been made for the visual form while similarly capturing the mapping from domain semantics to syntax of the visual form. During this discussion, attempts will be made to link back to the design concepts from the previous two chapters.

As part of this design process, there was an opportunity to talk with a variety of people interacting at different levels with the TCS. These included three design engineers who are responsible for implementing the user interface for interacting with the ground test article, one thermal engineer involved in evaluating and modeling individual component performance, and two flight controllers from space shuttle thermal systems who are targeted as space station ground-based controllers. Their comments will be discussed in relation to the applicable design feature(s).

## 6.2. Methodology

While there has been some mention of methodological issues in the development of the TCS overview display, this section will discuss in more detail the methodology used for building the overview display. Specifically, this will include the functional modeling (abstraction hierarchy development) building on the work of (Rasmussen, 1986; Vicente & Rasmussen, 1990; Woods & Hollnagel, 1987) and build on the problem-oriented approach in the previous two chapters.

### 6.2.1. Describing the demands of fault management

As discussed in Chapter 1, the first, high-level model guiding this work is a descriptive model of fault management with emphasis on the informational requirements for a user interface to support a human operator in fault management. To reiterate, the central issues are:

- to recognize, out of all the signal states and changes, which represent anomalies,
- to specify the different types of anomalies and the information processing requirements to recognize these classes of events,
- to differentiate between abnormal behavior (MP behavior that is different than desired system function) and unexpected behavior (MP behavior that deviates from the human operator's internal model of the system, and

72

- to differentiate between MP behavior and automatic responses to this behavior.

## 6.2.2. Functional modeling of the thermal control system

### 6.2.2.1. Abstraction hierarchy development

The first step in developing a function-based display that could support assessing TCS's status at a glance was to build a functional model of TCS based on Rasmussen's abstraction hierarchy (Rasmussen, 1986). More information can be found in (Vicente & Rasmussen, 1990; Woods & Hollnagel, 1987; Lind, 1991). This approach consists of an analysis of system objectives that determine higher-order functional properties that need to be presented to the human operator. Four basic levels have been identified and are used in this discussion:

(1) **functional purpose** – a specification of overall system objectives,

(2) **abstract function** – a description of the causal structure of the system,

(3) **generalized function** – a description of the system in terms of standard functions that instantiate the abstract functions above, and

(4) **physical function** – the components and their interconnections that carry out the system functions.

Another way to look at the relationships between levels of the abstraction hierarchy is that any one of the levels can be the focal point. It describes *what* is being performed. The level above describes *why* this is being performed, and the level below describes *how* it is being performed. These relationships are somewhat analogous to the goal/means approach to abstraction hierarchy development of Woods and Hollnagel (1987). In their approach, the activity being described at a particular level is trying to achieve some *goal* at the next higher level, and requires the activities from the next lower level as a *means* to achieve that goal.

According to Rasmussen (1986) the most important advantage of adopting this type of structure to analyze a system is that it provides a mechanism for coping with complexity. This is especially important for the current context of dynamic fault management. Additionally, for the fault propagation problem discussed in Chapter 2, faults tend to propagate upward through the hierarchy, while the reasons for normal functioning propagate downward (i.e., in order for a function at the abstract function level to be met, all of the inputs from the generalized function level must be satisfied.

One of the difficulties in this approach is how one goes from information about a particular system (schematics, functional specs, etc.) to a functional decomposition (i.e., the system described in terms of an abstraction hierarchy). In order to accomplish this task, the following steps were conducted. It should be noted that this was accomplished within a framework of working with a group consisting of three IS developers (knowledgeable on the TCS as well as their rule and model-based reasoning system) and two simulation developer (intimately involved in TCS functioning).

(1) Initial meetings were held which focused on gaining an understanding of system functioning and the approach being used to build an intelligent diagnostic system. This led to the writing of a functional description of the TCS (i.e., Chapter 3).

(2) A meeting was conducted to educate the IS developers on representation design and functional modeling, with examples from Vicente and Rasmussen (1990), Bennett (1991), T. Abbott (1989, 1990), Beltracchi (1989). The key elements included defining an abstraction hierarchy, its utility, and the applicability of this approach in designing an operator interface to the TCS and to their IS.

(3) Collaborative building of the abstraction hierarchy, using as information sources schematics and functional specifications, system performance data, and knowledge from the different group members.

Figure 27 contains a simplified version of the functional abstraction hierarchy developed for the TCS. It reveals several interesting aspects of this system. First, at the highest level, the goal of the system can be described as *isothermality* – to remain at the desired temperature setpoint. At first this may not seem intuitive, since the bulk of the discussion has concerned heat acquisition and/or rejection. However, if one thinks about the passive, adaptive nature of the system, it becomes more apparent. As heat load changes, the resultant change in pressure within the transport loop causes the BPRV to adjust the flow of vapor to the condensers *in order to maintain system pressure and temperature at the desired setpoint.*

The mappings between functional purpose and abstract function indicate that this goal is
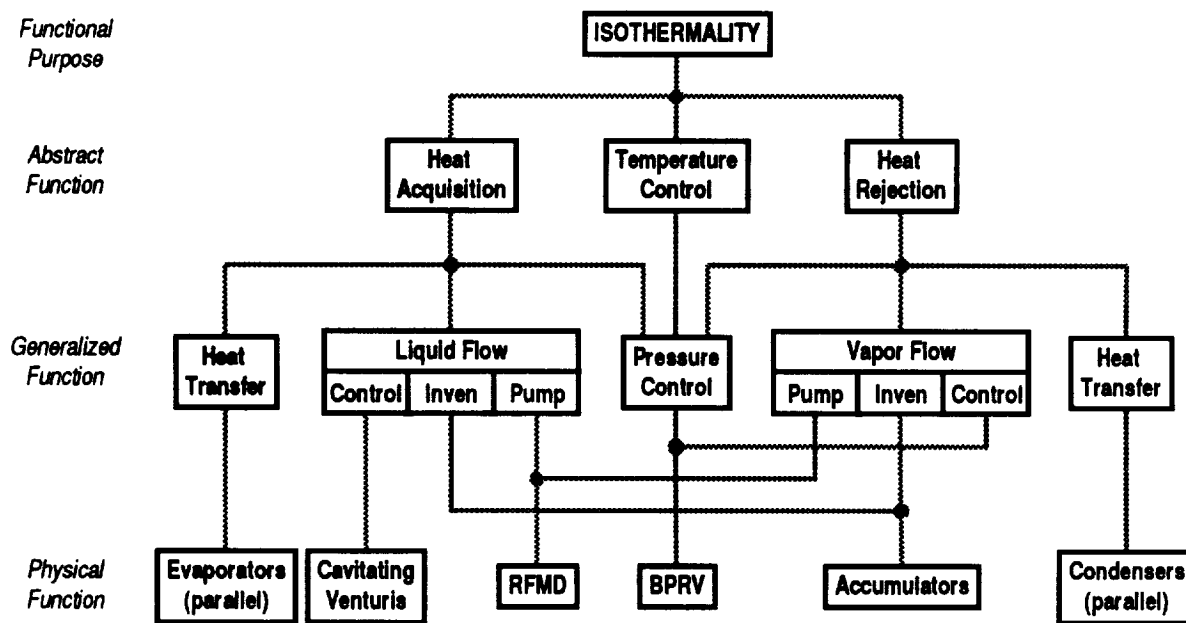


© 1992, Potter and Woods

Figure 27. Functional abstraction hierarchy.

accomplished by balancing the amount of heat acquired with that being rejected and controlling the temperature within the thermal bus. There is a considerable range over which the controlled flow of vapor to the evaporators can accommodate fluctuations in heat load. The mappings between physical function and generalized function reveal the multi-functional nature of some of the components. For example, as mentioned above, the BPRV controls saturation conditions (pressure/temperature) within the transport loop. This control also changes the vapor flow rate to the condensers, implying an inter-goal constraint (e.g., Woods & Roth, 1988b). However, these two goals are complementary. That is, reducing vapor flow rate to the condensers has the same direction of effect on saturation conditions as the increase in pressure.

### 6.2.2.2. Functional relationship identification

After the development of the abstraction hierarchy, the next step was to identify information requirements for the construction of the overview display. While Rasmussen's abstraction hierarchy is perhaps the most comprehensive framework for describing the semantics of a domain, previous work on functional modeling has been sketchy on a means to transcend from a functional model (abstraction hierarchy) to specific information requirements as a basis for display design. Bennett (1991) describes this as actually two separate goals:

> "First, an appropriate set of conceptual perspectives must be chosen, based on the semantics of the domain (the critical variables, the relationships between these variables, and the relevant goals and constraints). Second, these conceptual perspectives must be implemented (the domain information must be encoded) in graphic displays that allow the critical information to be easily extracted or decoded by the individual." (Bennett, 1991, p. 1208).

However, the work of Lind (1991) has focused on the use of multi-level flow modeling to represent information flow within a complex system. He describes the process as consisting of three steps: information analysis, design of means for generation of required MP information from available measurements, and planning of how this information should be presented to the operator.

To accomplish this step from conceptual perspectives to display design basis, functional relationships and available parameters to promote visualization of the goal-relevant system properties were identified. This was accomplished by constructing functional constraint relationships between performance indices (what evidence exists that function $x$ is being achieved?) and identifying conditions under which these relationships are valid (i.e., constraints) for each of the primary functions at the "abstract function" level. In addition, since one of the functions of this type of display should be to provide diagnostic information to the operator, a list of potential system faults that would impact these relationships was constructed. This was used later to check the choice of presentation mechanism selected for the representation of process behavior. From these constraint relationships, information requirements were derived.

**Heat acquisition.** Figure 28 presents functional relationships for the heat acquisition goal. As mentioned in previous sections, the key aspect of heat acquisition is *exit quality* (percentage of ammonia vaporized) of the two-phase return from the evaporators. Under maximum heat load, flow

rate to the evaporators is designed to produce 80% vapor to avoid superheating. For all heat loads less than maximum (representing normal operating conditions), the exit quality is proportionately < 80%. However, there is no direct measurement of exit quality, as this is still a research question in itself. Therefore, measured parameters (as well as potentially computed parameters) were identified to provide a foundation for insight into this higher-level performance metric. As this figure indicates, exit quality is a function of heat load applied to the system conditional on:

- heat loads within design limits,
- constant flow rate to the evaporators (by the use of cavitating venturis),
- saturated conditions within the thermal bus, and
- system integrity.

These constraints are violated by potential failures and lead to the information requirements discussed in section 6.2.2.3.

**Heat rejection.** Figure 29 presents functional relationships for the heat rejection goal. The critical aspect of heat rejection is amount of subcooling (temperature differential between saturated temperature and temperature of return flow from the condensers). Without adequate subcooling, the RFMD loses the required "pumphead" (end-to-end $\Delta p$) and loses system setpoint temperature control. Subcooling is a function of condenser flow rate and sink temperature (temperature of external surface

**Constraint Relationship:**

Exit Quality = f(Heat Load), given:

| **Potential Failures:** | **Information Requirements:** |
|---|---|

1. Heat loads within design limits → Excessive heat load(s) → Heat Load in terms of exit quality / Individual and aggregate exit quality

2. Constant flow rate
- Upstream pressure constant
  - ~ RFMD speed
  - ~ RFMD power
  - ~ Hot drum level
- No blockage
→ Loss of power to RFMD / Flooding in RFMD / Blockage in evaporator loop → RFMD power vs. speed / RFMD end-to-end $\Delta p$ / $\Delta t$ in evap loop / Cavitating venturis' flow coefficient

3. Saturated conditions
- Adiabatic piping
- Inlet from RFMD
→ Loss of insulation / Loss of saturation conds. in RFMD → $\Delta t$ in evap loop / RFMD temperature, pressure

4. System integrity
- Cavitating venturis
- Intact thermal bus
→ Leaking cavitating venturi(s) / Leak in thermal bus → Accumulator predicted vs. actual level

© 1992, Potter and Woods

Figure 28. Relationships between functional constraints and information requirements for heat acquisition.

of condensers) given:

- pressure control in condenser loop,
- vapor flow to condensers,
- adequate sink temperature, and
- system integrity.

Unlike exit quality, subcooling is a calculated parameter based on sensor values. Therefore, it can be directly presented rather than inferred.

**Temperature control.** Temperature control within the TCS is accomplished indirectly through change in the BPRV. the BPRV controls pressure to maintain saturated conditions (i.e., to control temperature). This is conditional on:

- BPRV operating correctly,
- system integrity, and
- energy balance between heat acquisition and rejection (i.e., not having more input to the evaporators than the condensers can dissipate).

As was mentioned in the abstraction hierarchy development section, a balance must be maintained within the system. It is possible, for a variety of reasons, for one to exceed the other. Within limits, the function of the BPRV is to adjust to variations in the heat acquisition loop by varying the amount



**Constraint Relationship:**

**Subcooling = f(flow rate, sink temp), given:**

**Potential Failures:**

**Information Requirements:**

1. Pressure control in condenser loop
   - BPRV operating correctly
   - Pressure differential in condenser loop
     ~ RFMD speed
     ~ RFMD power
     ~ Hot drum level
     ~ Minimal NCG buildup

Failed BPRV
Loss of power to RFMD
Flooding in RFMD
NCG buildup

BPRV upstream temperature
BPRV position (potentiometer)
End-to-end Δp
RFMD power vs. speed
Accumulator level

2. Vapor flow to condensers
   - BPRV operating correctly
   - No blockage

Failed BPRV
Blockage in condenser loop

BPRV info (from above)
Δt in condenser loop

3. Heat transfer capability
   - Adequate sink temperature
   - Adiabatic piping

Radiators improperly positioned
Loss of insulation

Δt in condenser loop

© 1992, Potter and Woods

Figure 29. Relationships between functional constraints and information requirements for heat rejection.

of vapor flow to the condenser loop (and thus the amount of heat being rejected).

### 6.2.2.3. Information requirements

**Excessive heat load.** The critical heat acquisition parameter of exit quality actually can be decomposed into two components. First is the aggregate exit quality of all evaporators after the return lines are recombined. This is important as a global indication of amount of heat being acquired. Second is the exit quality of each individual evaporator (i.e., the maximum of 80% applies to individual as well as aggregate return). It is critical that individual exit quality not exceed the design maximum in order to prevent evaporator overheating. However, the aggregate value may hide important behavior. For example, four evaporators could be yielding 50% exit quality and one yielding 100%, resulting in an aggregate value of less than 80%. Despite the acceptable aggregate value, one evaporator is still in danger of overheating. Based on this, an indication of aggregate and individual evaporators needs to be presented. However, individual evaporator conditions need only be displayed if they deviate significantly from desired or expected state. Additionally, even though the test-bed configuration has only five evaporators, SSF will have over 20, prohibiting comprehensive coverage. Therefore, display design requirements include a depiction of aggregate value as well as maximum and minimum of the individual values.

**Nonconstant evaporator flow rate.** As previously mentioned, the cavitating venturis provide constant flow rate specifically tuned to the maximum heat load for each evaporator. The critical parameter for constant flow rate is the cavitating venturi's flow coefficient, defined by Equation 1. As long as the flow coefficient is ≤ .85, changes in heat load will not alter flow rate; the relationship between heat load and exit quality will be valid. However, above this limit flow decreases, resulting in an underestimate of exit quality. Events which would cause an increase in this flow coefficient include changes in RFMD (e.g., speed, power, or liquid level), BPRV failure, and leaks in the system. The three parameters in this equation are computed by the IS based on a model of the TCS and on measurements of current conditions within the thermal bus. Therefore, changes in flow coefficient are included in the heat acquisition display to highlight conditions in which the exit quality indicator are inaccurate.

$$\text{flow coefficient} = \frac{\text{(outlet pressure)} - \text{(saturation pressure)}}{\text{(inlet pressure)} - \text{(saturation pressure)}} \tag{1}$$

**Loss of saturated conditions (to evaporators).** Another condition for the linear relationship between exit quality and heat load is the presence of saturated liquid within the evaporator inlet pipes. Since heat is acquired through vaporization (and not temperature change), if exit quality is < 100%, the temperature differential (Δt) between the setpoint temperature and output of the evaporators should be approximately zero. This Δt would only be non-zero when:

- exit quality reaches 100% (and additional energy acquired results in a positive Δt) or
- liquid flow to the evaporators is not at saturation point.

The former condition could potentially provide insight into excessive exit quality in the absence of abnormally high heat loads (e.g., blocked evaporator or cavitating venturi, non-adiabatic piping).

Unfortunately, differentiating between these two conditions is not straightforward. The variability in the saturation conditions of the incoming liquid prevents the setting of any static limits to indicate excessive $\Delta t$. However, the IS computes a dynamic $\Delta t$ parameter that accounts for changes in saturation conditions and is used by the IS as a means to detect anomalies in the evaporator loop. Therefore, this dynamic $\Delta t$ is used as a means to highlight conditions of excessive exit quality. This can provide confirmatory information when exit quality exceeds the maximum due to excessive heat load *or* an indication of a fault when heat load is normal but $\Delta t > 0$.

**System integrity.** As heat load changes, changes in the liquid/vapor balance in the RFMD are compensated for by two accumulators. While by design these accumulators can accommodate a wide range of heat loads, they can also compensate for faults (such as leaks) until all inventory is exhausted. Therefore, they provide supporting information for other functions within the TCS. Information extraction requirements for an inventory display include:

- an indication of excessive levels (i.e., too full or too empty) and
- mechanisms for highlighting loss of inventory (i.e., slow leak).

The IS simulates accumulator position based on conditions in the thermal bus (e.g., present heat load, sink temperature, valve positions, flow rates) to provide an estimate for comparison to current measured level. This is referred to as mass gauging. This value is propagated instantaneously to result in a predicted value, and work is being performed to propagate this value in real time to provide an expected value (since it takes several minutes for inventory to be transported through the bus, and consequently for system changes to impact all components).

The instantaneous simulated value provides a predictor, although no precise lead time is actually specified by this prediction. The behavior of this display is analogous to other forms of predictive information such as compensated level (Woods & Roth, 1988b). The real time simulated level will provide an indication of actual vs. expected to highlight anomalies such as a slow leak. In this manner, such faults could be detected much earlier than if allowed to continue until other system functions were affected.

**Subcooling margin.** As discussed in Chapter 3, the TCS requires 5 - 10°F subcooling margin for stable performance. Subcooling is a relationship between temperature and pressure, defined as the difference between the current temperature and the saturation temperature for the pressure of the current temperature. The critical aspect of subcooling is that it is an indication of temperature change conditional on pressure. Unlike exit quality, subcooling can be directly computed from available sensor values. Loss of subcooling can be a result of increased sink temperature, loss of insulation (and thus temperature increase in the condenser return), or blockage in the condenser loop. As subcooling is lost, RFMD performance will be affected. Specifically, end-to-end $\Delta p$ will be lost and the system will re-establish a higher setpoint temperature.

**Loss of saturated conditions (system-wide).** The BPRV is the primary component to control saturation conditions throughout the TCS. As mentioned in Chapter 3, the BPRV controls system pressure to maintain saturation and, thus, temperature. Loss of BPRV control will result in loss of

saturation and loss of temperature setpoint control. Therefore, it is important to provide insights into the functioning of this device. Available parameters include BPRV position (based on potentiometer reading) and upstream pressure (based on sensor). Both of these parameters can be transformed into temperature (based on BPRV calibration tables and temperature/pressure saturation equation, respectively) to provide comparative indications of saturation conditions within the thermal bus.

**Energy balance information.** As indicated in the abstraction hierarchy, one of the critical system functions is to balance heat (or energy) acquired with that rejected. More specifically, it is the capabilities to adapt to varying amounts of heat load being imposed on the system. For example, an increase in sink temp will eventually result in the condensers being unable to dissipate the heat load being applied. As mentioned above, temperature in the evaporator return can increase with an excessive heat load. However, the primary concern is whether this affects the system setpoint temperature as considered from conditions upstream of the BPRV. Thus, it is important to provide indications of thermal conditions in the evaporator loop as well as system-wide to provide insights into the ability of the system to adapt to input changes.

## 6.3. Display design description

### 6.3.1. Function-based display

#### 6.3.1.1. Overview

Figure 30 presents the function-based display for the TCS. As the 'status-at-a-glance' display was organized by the physical structure of the TCS, the function-based display is organized around the various functional properties of the system. The discussion will be organized around the system functional properties. In general, the approach is to depict deviations from nominal. In several cases (to be described in more detail below), nominal is a computed value based on the model-based system. Analog and digital forms of presentation are used to provide qualitative and quantitative indications of system performance. Deviations from nominal are highlighted by color-coding of the border around the display units and color coding of the specific analog form and digital data display. For example, this figure has the bottom-left display unit (exit quality/heat load) highlighted.

#### 6.3.1.2. Temperature control within the TCS

This functional property of the system has been divided into two components – evaporator loop temperature and system/setpoint temperature (temperature upstream of the BPRV). The upper-left display unit depicts information about evaporator loop temperature. This refers to the temperature change of the ammonia throughout the evaporator loop. Rather than presenting information about each evaporator, this display has been designed to provide temperature information about the total liquid/vapor outlet flow from the evaporators (to the RFMD) and the maximum and minimum individual evaporator temperature conditions. This is because, despite only having five evaporators in the ground-based test article, the flight article is planned on having approximately 20.

Each of the three bar-graphs is plotted against expected temperature since system transients result in expected deviations from the setpoint value of 70°. This expected value is a real-time computation from the model-based system. Since the "max" and "min" graph are adaptive (i.e., they can, at any given time, be representing any one of the evaporators), the label of the evaporator being represented is shown below the graph (e.g., refer back to Figure 24 to see an example of this change).

System/setpoint temperature refers to the temperature upstream of the BPRV. This refers to the ability of the system to maintain the predefined target (either 70° or 35°F). For this system goal, three parameters are presented in the upper-right display unit. First is the measured value based on the thermocouple (sensor) between the RFMD and BPRV; second is the predicted value based on pressure sensor at the BPRV transformed (by the relationship between pressure and temperature based on the saturation curve) into temperature; third is the calculated value based on the current position of the BPRV (based on valve position) transformed into temperature as well. They are all presented in terms of temperature to facilitate comparisons. These three parameters are presented together to provide complementary representations of setpoint temperature.



© 1992, Potter and Woods
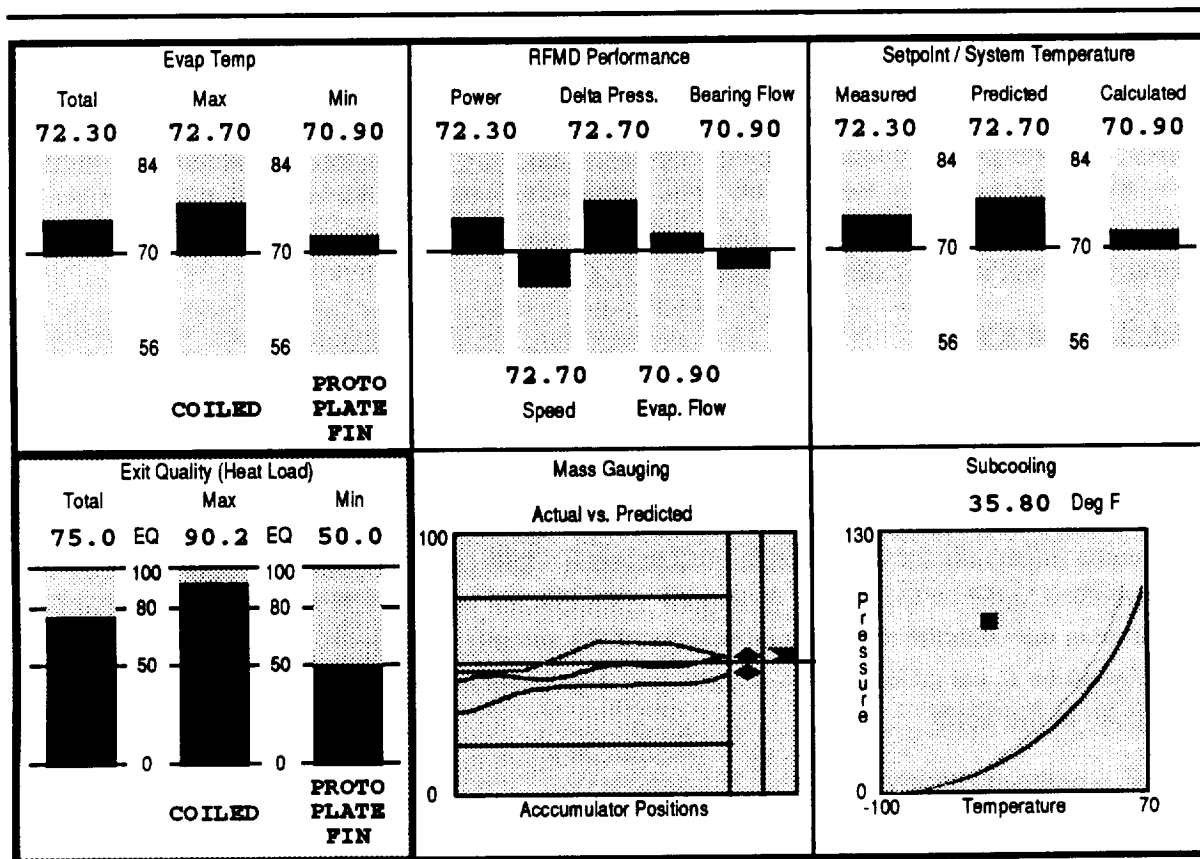
Figure 30. Function-based display for the thermal control system.

### 6.3.1.3. Heat acquisition

Heat acquisition is expressed in terms of exit quality (percent vapor) of the ammonia from the evaporators and is presented in the lower-left display unit. This is derived from the heat load being applied to each evaporator (as well as the combined heat load of all evaporators), the heat transfer capabilities of each evaporator, and the constraints on this relationship described earlier in this chapter. In this manner, heat acquisition is expressed in terms of percent of maximum, normalized across evaporators with different design capacities. Like the evaporator temperature display described above, the heat acquisition display depicts the overall (combined) and the maximum and minimum (individual) evaporator conditions. Therefore, it is expected that these two displays will be complementary in their information presented.

### 6.3.1.4. Heat rejection

Heat rejection refers to the functioning of the condensers in radiating heat to space. It is expressed in terms of subcooling, which is the difference between the current temperature of the condensate return and the saturation temperature corresponding to the condensate return pressure. The critical regions of 5 and 10° subcooling margin are indicated by the two saturation curves drawn on the graph.

### 6.3.1.5. RFMD performance

To provide insights into the functioning of the RFMD, five critical parameters are presented. These include: RFMD power, rotational speed, end-to-end Δp, flow rate to the evaporators, and bearing flow. Except for the power, these are the same parameters included in the 'status-at-a-glance' display. They are all presented as deviations from expected, where expected is again based on a real-time computation from the model-based system.

### 6.3.1.6. Mass gauging

Mass gauging refers to the liquid and vapor inventory in the accumulators. Levels for the two accumulators are presented along with history strip charts. The strip charts are designed to provide greater information as to the direction and rate of change for these parameters. In addition, a predicted level (an instantaneous computation from the model-based system) is presented for comparison (especially for the detection of slow leaks). This predicted value is instantaneous in that it is computed based on the current conditions in the thermal bus. It does not propagate in real time (i.e., it does not consider the temporal aspects of the system) and thus is not a predictor of where level should be at the present time. Rather, it is a predictor of where accumulator level will be at some point in the future.

### 6.3.1.7. Interim summary

Some of the concepts illustrated in this display design include:
- adaptive display formats to provide an overview of system functioning while highlighting anomalous conditions,

- the use of different types of model-based computations (real-time and instantaneous) to provide evaluative context for interpreting system behavior,

- generation of higher-order parameters to provide an integrative view of MP behavior,

The organization of this display based on a functional analysis of the system provides a mechanism for capturing the temporal cascade of events as the impact of an anomaly spreads throughout the system. For example, an increase in sink temperature will first be indicated by an increase in condensate return temperature (loss of subcooling). The uncondensed vapor returning to the RFMD will impact end-to-end $\Delta p$ (in "RFMD Performance" display unit) and then measured system temperature (in "Setpoint / System Temperature" display unit).

## 6.3.1.8. Insights from subject interviews

**Bias towards schematic displays.** There was a tendency for a preference for the old 'status-at-a-glance' display based on comments that it [schematic displays with digital data] was "more like I'm used to," "provides more of the details," and "easy to see what's going on." It is important to consider this finding in conjunction with the next finding.

**Focus on a raw sensor level view of the system.** There was virtually no mention of any description of the system in other than a description in terms of raw sensor values. Even when queried, no one was able to describe any higher-order parameters they use to conceive of the system. One subject agreed that people tend to talk about this system (and other complex systems) in terms of higher order system properties, but was not able to verbalize what they were. He did indicate, though, that these properties should be a part of the overview display.

For example, one person commented that if he knew the input flow rate and temperature [to an evaporator], the heat load being applied, and the outlet temp, he knew how the evaporator was performing. He also said that he knew exactly what the flow rates and heat loads should be for each evaporator. But note how this requires:

- extensive experience with the particular configuration,

- demands on operator memory instead of using displays as an external memory, and

- continual comparisons and manipulations of digital data.

All of this information, however, is captured in the derived parameter *exit quality*.

**Inadequacy of trend arrows to convey dynamics of the system.** As expected, the mapping of parameter rate of change into three discrete states of the trend arrows was not well received. One comment reflects this: "It's distracting to see the arrows change in 90° increments − because you blink and the arrows are in a different position." This is partly due to the lack of continuity in the incoming data (as data is received every five seconds). Also, as discussed in Chapter 5, this is primarily due to the underspecification of the temporal information to be conveyed.

**Heavy reliance on trend information.** As an addendum to the last item, there was a unanimous mention of the importance of trend information in monitoring and controlling the TCS. Specifics

were usually discussed in the form of plots of one or more parameters over time. Comments also indicated that it is the details of such a graph and the ability to review historical data that are important. Details such as: shape of the curve (how high did the parameter reach before recovering) and temporal sequence of behavior (which parameter started to increase first, how much time elapsed between events, exactly when did this change start) seem to be critical to understand the physics of the situation that produced the particular result.

It is important to note that this type of information is substantially different than the information in the trend arrows. The arrows only depict relatively current behavior (what is happening with this parameter recently); they do not allow for any retrospective analysis nor do they facilitate comparisons between parameters.

**Deviations from nominal.** The approach used in the function-based display of anchoring analog data presentation based on deviations from nominal was viewed as in line with how the subjects tended to view things. Along these lines, several of the subjects indicated a need for color coding of digital data display for the old 'status-at-a-glance' display. However, in accord with results from modeling complex systems (Wickens, 1992), it was realized that static, pre-defined threshold limits would not be applicable and that it would be extremely difficult to develop adaptive thresholds.

## 6.3.2. Temporal information display

### 6.3.2.1. Overview

The temporal information display, depicted in Figure 31, is composed of several units: an overview timeline, a current message list, and a past message list. Each will be discussed below, as well as how they are coordinated.

### 6.3.2.2. Overview timeline

The overview timeline provides an overview of events in the MP and activity in the IS. This presents the most recent hour of activity. The timeline is separated into three columns. The left column represents time in order to anchor all activity to a reference point. The middle column contains indications of MP events; the right column indicates IS activity. Each event or activity is indicated by a tickmark on the overview timeline (and, as will be discussed in the next section, by a message in the message list).

In order to represent criticality of events, the tickmarks are coded by length (i.e., there are four "sizes") and redundantly by color. The longer the tickmark, the higher the criticality of the message. Medium and high criticality events are denoted by yellow and red, respectively. Shorter tickmarks are always placed in front of longer ones to minimize hidden information. Event density is conveyed through the density of tickmarks on the timeline, as this is a temporally-based representation of activity.

As new messages are received by the timeline application, an appropriate tickmark is created at the bottom of the overview timeline. On an interval equivalent to the data update rate (every five seconds), the ordinate coordinates of the tickmarks are incremented 1/720 of the height of the timeline.

### 6.3.2.3. Current message list

The "current messages" portion of the temporal information display (bottom portion of Figure 31) is a non-scrollable text window with two columns of messages. It is not scrollable so that there is always a window into incoming messages; the two columns are analogous to those in the overview timeline portion of the display. As a new message is received, it is added to the bottom of this window.

One of the primary differences between this approach and typical message lists is the fact that the current messages window is updated on the occurrence of a new message *or* a period of inactivity. That is, if a prespecified amount of time elapses, a blank line is added to the message list. This



© 1994, Scott S. Potter
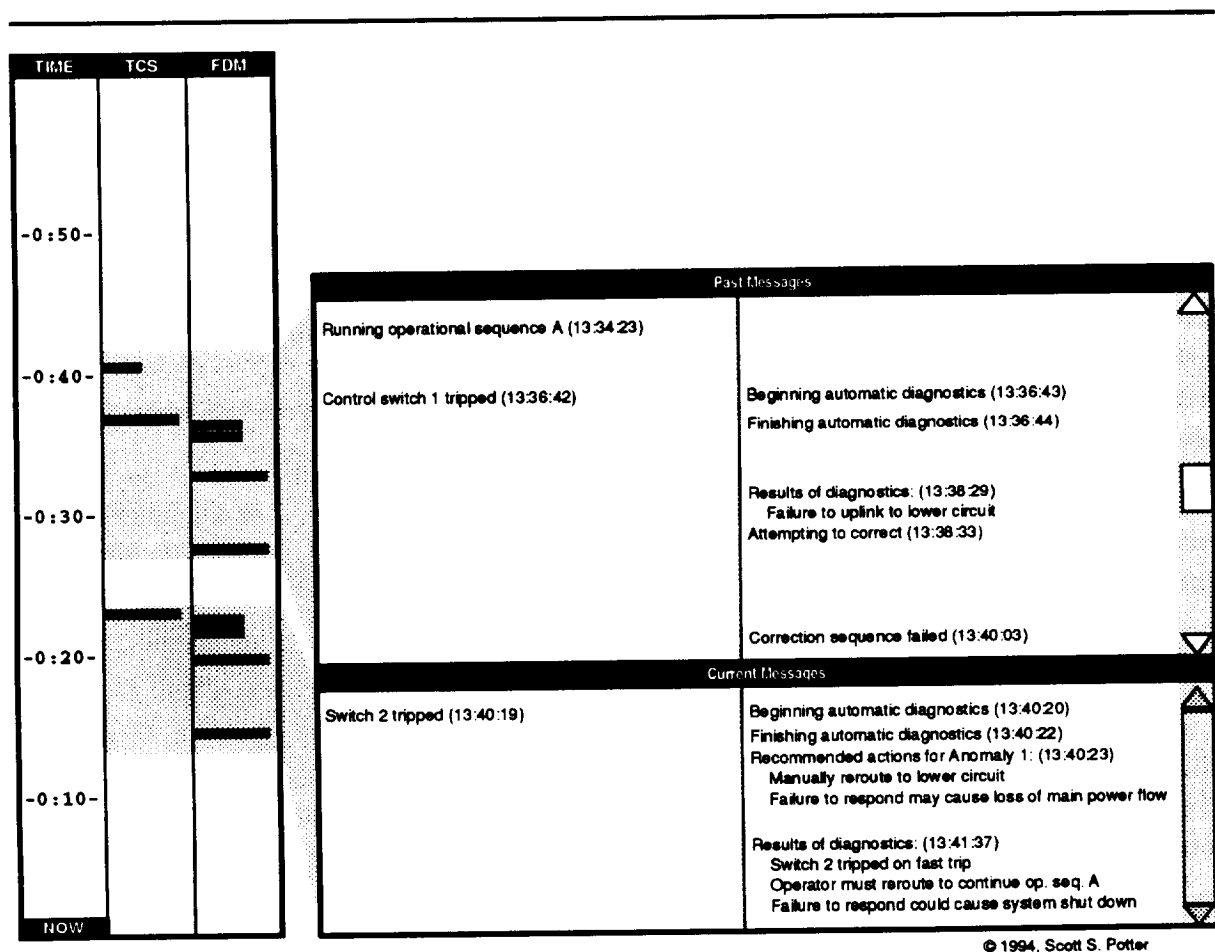
Figure 31. Temporal information display.

provides greater similarity between the overview timeline and the messages (as both are analogous to a timeline), a representation of event density, and landmarks to aid navigation within the messages. As user interface technology advances, the vertical spacing between events can be more continuous (as opposed to the present categorical approach). As incoming messages are posted in this window, its capacity will become exceeded. At that point, old messages are passed to the past message list.

### 6.3.2.4. Past message list

The "past messages" portion of the temporal information display (top portion of Figure 31) is a two-column text window similar to the current messages window. However, it is scrollable to allow for browsing through the entire hour's worth of messages, and twice the size of the current message window to provide a greater view of activity. This window receives a message whenever the capacity of the current message window is exceeded. It is important to note, then, that this window can not scroll down to the most recent messages – it is limited to "past" messages only. The distinction between past and current message windows is important since it provides a mechanism for reviewing past events without being interrupted by (or unaware of) incoming messages.

### 6.3.2.5. Coordination within temporal information display

There are several means for coordination within this display to enhance its usability. First, the tickmarks in the overview timeline display are "clickable" (i.e., clicking the left mouse button activates) to serve as a high-level scroll bar. Clicking on a tickmark causes the past message window to scroll so that the message of interest is at the top of the window. (These tickmarks are actually X-Windows buttons with no labels.)

Second, as indicated in the figure, the period within the overview timeline that is presented in the current as well as past message lists is highlighted on the timeline. As event density changes and/or as one scrolls around within the past message list, this highlighting will change in size and/or vertical location, respectively.

Third, the two message windows can be "joined" by scrolling the past window to the bottom of its messages. This provides a means for viewing a greater number of contiguous messages simultaneously.

Fourth, there are two mechanisms for providing an explanation for a particular diagnosis. The first is achieved through coordination between the two columns of text within a message list. If an IS diagnosis (right side) is selected (left mouse button), the TCS message(s) (left side) pertaining to the rule that led to the diagnosis are highlighted (as shown in Figure 19 of Chapter 4). The second type of explanation is graphical, through a plot of these same parameters over time. This is accessed by selecting the diagnosis message with the right mouse button.

Fifth, the operator is not limited to the most recent hour of messages to view. As messages exceed the time limit for the overview timeline, they are written to a log file which can be called up and displayed. Each log file contains one hour of messages and can be displayed on top of the current

temporal information display. The behavior of the log file display is exactly the same except that messages and tickmarks are static.

## 6.3.2.6. Interim summary

The temporal information display overcomes many of the problems inherent in typical message list approach by the use of:

- overview timeline to provide a "longshot" view of events and activity,
- overview timeline and temporally-based message list to depict temporal sequence and density,
- separation of current and past message windows to allow for the ability to review old messages while keeping informed of new activity,
- coordination between the message windows and overview timeline to improve visual momentum within the display space,
- graphical linkage between IS diagnoses and MP causal events to provide explanation capabilities.

**Overview timeline.** This provides a macro-level view of the events of the previous hour in order to convey the *temporal sequence and density* (Sect. 4.2). Used independently of the message windows, it provides landmarks of where events occurred, how many events occurred, how long ago they occurred, and how quickly they occurred. In conjunction with the message window, it provides a mechanism to navigate to the previous messages in an attempt to overcome the problem of *temporally fleeting data* (Sect. 4.3).

**Current message window.** Since the temporal aspect of messages is preserved to some degree in this representation (by vertical spacing of messages), temporal sequence and density is further preserved. The design decisions of (a) retaining one hour of messages and (b) when to post a blank line (indicating no activity) were based on an analysis of the *temporal characteristics of the physical system* (Sect. 4.4). The two mechanisms for depicting relationships between MP events and IS diagnoses (highlighting of TCS messages in left column of window and providing a historical plot) attempt to depict *the temporal cascade of events* (Sect. 4.5). Certainly, though, this is an area that could be pursued further.

**Past message window.** The separation of current and past message windows allows the operator the freedom to explore the entire display space of messages without missing new messages, which addresses the problem of temporally fleeting data.

## 6.3.2.7. Insights from subject interviews

**Ineffective use of message lists.** The general approach to using message lists is in the form of alarm lists (how many system parameters are out of tolerance) without any indication of:

- when the parameter recovered,
- what anomalies have occurred in the past,
- what TCS events have resulted in the "intelligent alarms" (IS diagnoses).

However, this approach only conveys present conditions and does not provide for any analysis of event sequences or temporal dependencies.

**Complementary nature of message lists.** There was a desire for the message list to complement the information presented on the 'status-at-a-glance' display (e.g., to have messages about parameters not included on the 'status-at-a-glance' display). This was expressed best as "I need the message list to tell me what I can't see" . . . "anomalies will be easy to detect on the function-based display."

## 6.4. Coordination between displays

Figure 32 shows the function-based display together with the temporal overview display to form what will be referred to as the *functional overview display*. This display provides a joint view of the MP and IS, with the ability to focus on either one. However, it should be emphasized that each of the views are not solely a "MP display" and an "IS display". As this work has shown, information from each is used as context to help in interpreting the events of the other.
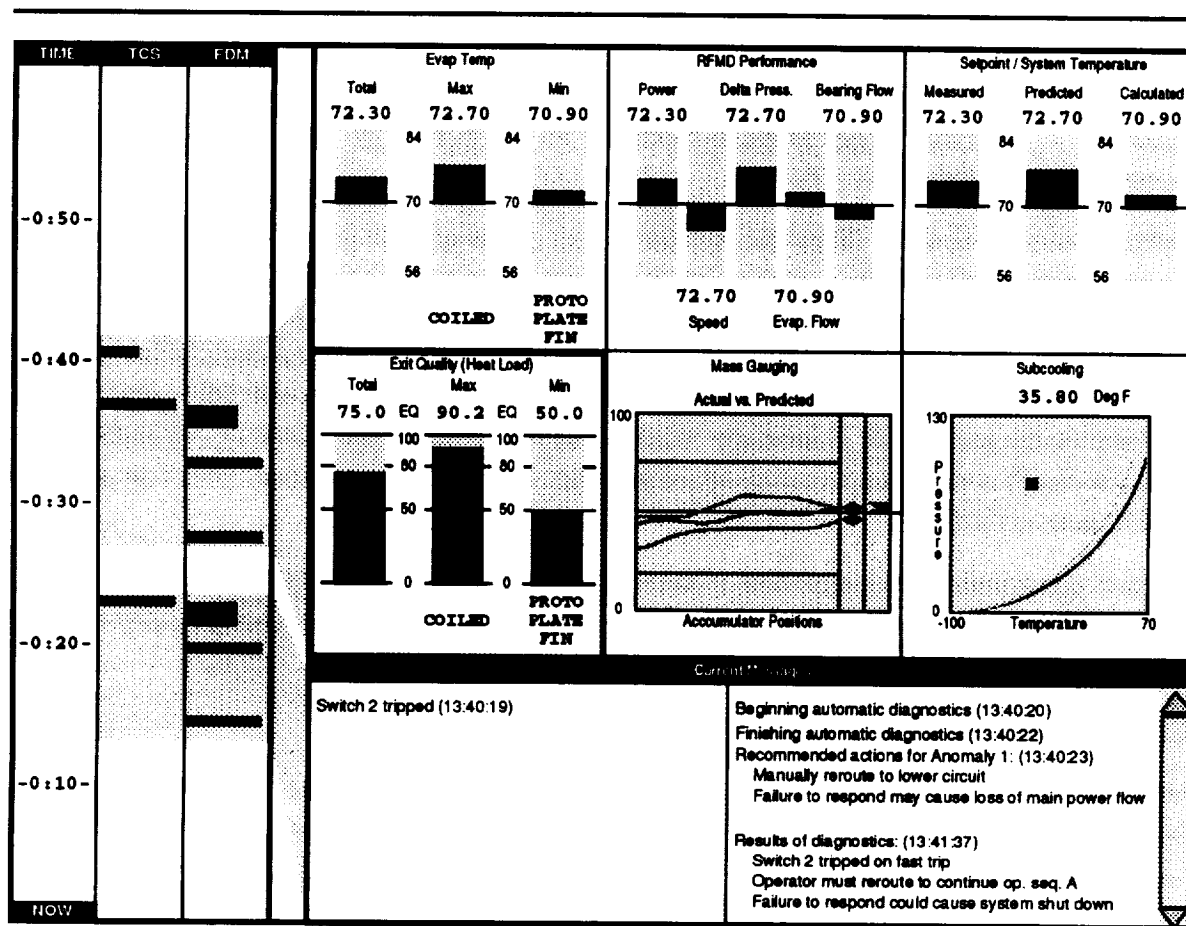


© 1994, Scott S. Potter

**Figure 32. Functional overview display for the thermal control system.**

One of the design features of this functional overview display is the sharing of CRT real estate between the two views. Figure 32 depicts the display in "real-time" mode, where the focus is on the current behavior of the MP (through the function-based display) and incoming messages being posted to the current message window. The permanence of the overview timeline display provides a constant cue of past events and activity. In Figure 33, the past message window has been brought to the front to allow the operator to review previous messages, while the top portion of the function-based display provides the most critical information about current conditions (i.e., temperature control and RFMD performance metrics).

Another capability that has been included in this design is a "replay" mode. This is the ability to select a message in the past message window as a starting point and replay data from that point through the function-based view. This, of course, requires that the sensor and computed data be saved in a buffer. Wickens (1992) mentions this as a powerful tool to allow the operator to recover an accurate picture of the progressive series of events. One critical issue in implementing a replay capability is to allow the operator to select the speed of replay. Given the proposed monitoring



© 1994, Scott S. Potter
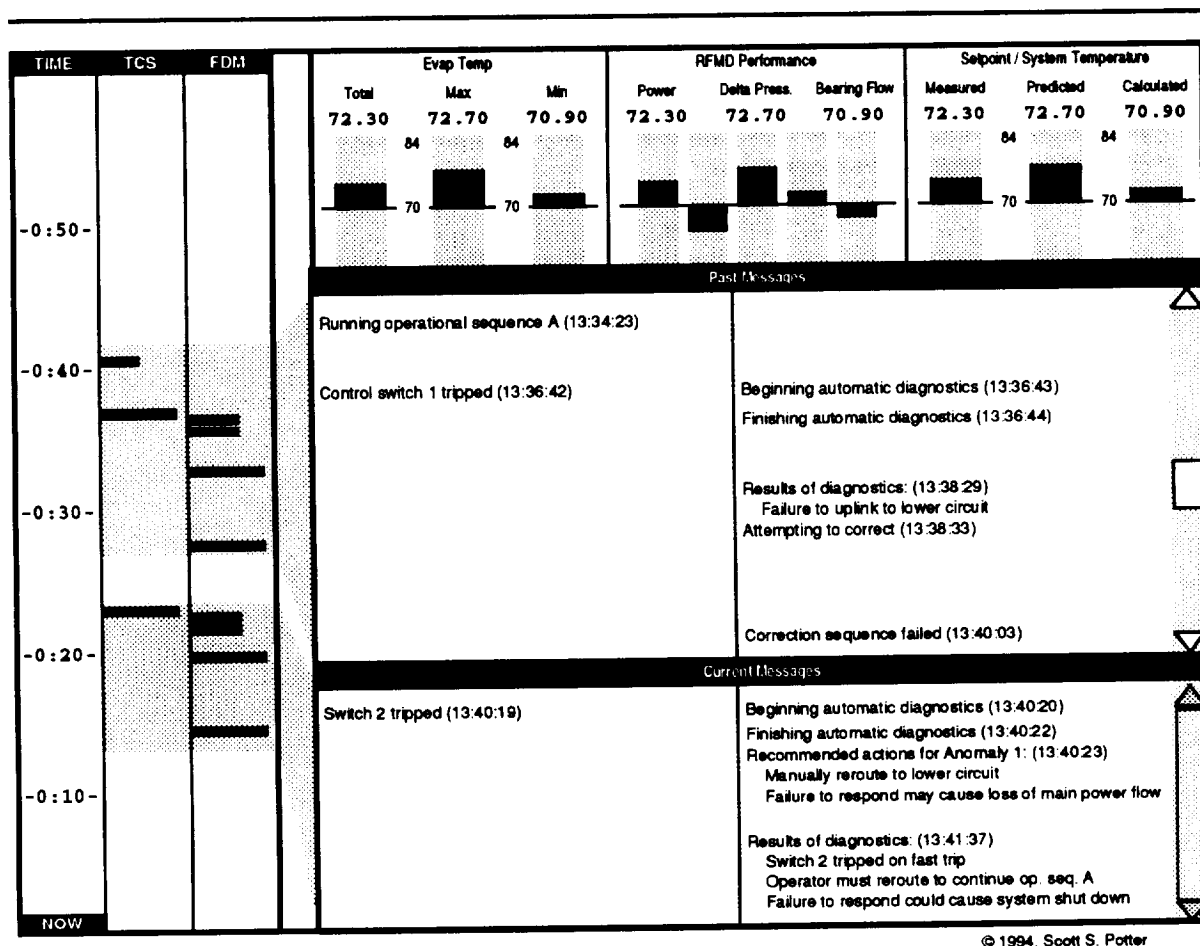
Figure 33. Functional overview display in "review" mode.

strategy of future space operations (one operator for extended periods of time) there is an increased probability of missing a critical or interesting event and needing to replay the sequence of events.

## 6.5. Discussion

To reiterate, the primary emphasis of this design effort has been to *integrate* data sources to enhance the informational value of the displays. As mentioned in Chapter 1, the work of Shafto and Remington (1990) on previous IS development effort for the TCS has highlighted the need for this emphasis. In this system, there were two primary displays residing on separate CRTs – the expert system screen (ESS) and the graphics schematic screen (GSS). One of their findings was that subjects did not make extensive use of the independent representation of the IS results (in the ESS). Diagnoses were validated by referring to the physical schematic (the GSS). Information integration has been accomplished in the present design on several dimensions:

- the function-based display makes use of IS-generated computations as context for interpreting MP behavior,

- the temporal information display depicts relationships between MP events and IS diagnoses, and

- the concurrent display of the function-based display and current message window provides a complementary view of the events of the two systems (MP and IS) – a graphical indication of MP behavior on the function-based display followed by a textual presentation of IS activity on the temporal information display.

# 7. Conclusions and Recommendations

## 7.1. Introduction

This chapter will attempt to link the attributes of the display design (as presented in Chapter 6) to the underlying issues in the weaknesses of typical approaches presented in Chapters 2, 4, and 5. To begin, the next section will re-define the research goals and context of the work. This will include commonalities identified in the case studies, the approach used to overcome these limitations, and the design goals. Next, insights gained from the design process will be presented, including a discussion of the design attributes with respect to design concepts presented in Chapters 4 and 5. These sections will provide a basis for future research and design work, the concluding section of this chapter.

## 7.2. Recapitulation of research goals

### 7.2.1. Commonalities in real-time IS development work

As Chapter 1 outlined and the appendices describe in more detail, there was a high degree of similarity between the types of development projects investigated. To reiterate the primary weaknesses:

- digital data as the primary means to convey MP system status. As shown in Chapter 5, digital data does not contain any graphic properties to convey emergent properties and presents information at the raw, sensor level without any integration, abstraction, or normalization to provide higher-level informational properties.

- static physical topology schematic displays as the background for presenting the digital parameter values. While these are useful for conveying the physical layout of the MP, they have not been adapted to depict system status (through dynamic coding) and do not emphasize functional relationships between components.

- chronologically ordered message lists as the means to convey information from the IS. As discussed in Chapter 4, this approach vastly underspecifies the temporal issues in systems, fails to establish a relationship between diagnosis and causal events in the MP, and does not support the style of interaction proposed for flight conditions (a "generalist" rather than a "specialist").

- IS primarily functioning as a parallel, independent problem solver. Very little attention was given to using the computations and reasoning to assist the human operator in visualizing and maintaining awareness of MP behavior.

The primary result from Phase I was that, despite different approaches (i.e., development tools, IS architecture) and applications, HCI commonalities lent themselves to further investigation and a high degree of generalizability of design concepts and specifications.

91

## 7.2.2. Approach to overcome HCI problems

In general, these case studies revealed a need to break down the communication barriers between the MP, the IS, and the human operator and improve the operator's ability to assess the state of the MP and track the IS as it responds to changes in the MP. The approach used toward this goal has been to:

- adopt a generic model of human information processing in dynamic fault management as a guiding mechanism for design,

- identify and formalize the critical temporal, functional, and coordinative issues in human-IS interaction in dynamic fault management as a basis for information requirements of an operator interface,

- construct a functional decomposition of the TCS to identify the critical functional relationships, properties, and parameters of the particular system under investigation,

- integrate the previous three steps into a dynamic representation of the MP and IS consisting of a function-based display to provide an enhanced visualization of events and anomalies within the MP and a temporal information display to provide a historical overview of MP events and IS activity, a temporal-based representation of these events and activity, and to establish causal relationships between MP behavior and resulting IS diagnoses, and

- coordinate these two displays to jointly serve as a functional overview display to depict system status "at a glance."

## 7.2.3. Design goals

As the primary focus of this work has been on the development of HCI tools for improving the informational content of the representational design for dynamic fault management, it is important to define the goals of the design effort. These will be phrased in terms of questions addressed by the research:

- can the temporal characteristics of events and activity within the MP and IS be captured and represented through a design in order to assist the operator in the tasks of monitoring for, detecting, and diagnosing anomalies?

- can the functional modeling approach of Rasmussen be successfully applied to a complex, real-world, passive system such as the TCS? (i.e., the TCS contains inherent differences from the system investigated by Vicente & Rasmussen, 1990)

- what gaps are there in this approach that need to be filled? (i.e., what "leaps of faith" or steps requiring "extensive experience in HCI" exist?)

- can these approaches help in the development of an overview display for a complex system such as the TCS?

## 7.3. Insights and contributions from the design process

The organization of this section is analogous to the design goals just outlined. The purpose of this is to discuss the major insights gained from the modeling and design work, focusing on the successes achieved and difficulties encountered.

### 7.3.1. Temporal representation of MP events and IS activity

This work has shown the importance of temporal information in dynamic fault management and outlined concepts for designing a temporal representation for a complex system such as the TCS. As shown in Chapter 4, temporal information is generally ignored in current representations, yet can be a very valuable tool for diagnosis. Given the even-driven nature of fault management, highlighting critical events and showing relationships becomes a critical issue for improved communication of system status to the human operator.

One of the strengths of this temporal modeling approach is that it is independent of the particular application domain. This same approach could be used in other aerospace applications, nuclear power, or chemical process control.

Some of the limitations would be:

- systems with a very short temporal dimension (e.g., electrical power systems) would not benefit as much from this approach since there are not the time lags and dependencies.

- additional work would be required to apply this concept to a larger system (such as the entire space station or a nuclear power plant) where the number and type of messages would be increased. In these situations, more attention would have to be given to the granularity issue in Section 4.6.

### 7.3.2. Utility of functional modeling in overview display development

This research has extended the functional modeling approach of Rasmussen (1986) to a complex, real-world system and demonstrated its utility in specifying functional relationships within the application domain. The use of Rasmussen's (1986) abstraction hierarchy to decompose the TCS proved to be an effective way to describe the system and identify critical functional relationships. It resulted in a "straw man", against which design ideas needed to be bounced as well as a "meeting of the minds" among the diverse members of the design group.

Some of the critical lessons learned from this process include the need for:

- diverse resources (people with different backgrounds, areas of expertise). Without individuals possessing extensive experience with the system it would be impossible.

- one group member (in this case, the author) to serve as a teacher of the process to the domain experts, and the need for examples from which to draw, and

- extensive time investment (once again, by the author) in becoming sufficiently familiar with the system to be able to serve as the "moderator" for the modeling effort. It was critical to be able to query the individuals about domain-relevant suggestions proposed during this process.

As mentioned in Chapter 6, much of the functional modeling literature (Rasmussen, 1986; Vicente & Rasmussen, 1990; Mitchell & Saisi, 1987; Beltracchi, 1989; Bennett, 1991) fails to focus on the process of transforming a functional decomposition into information requirements and display design. Thus, one of the main contributions of this work is the demonstration of the utility of

constraint relationship identification as an intermediary step in the display design process. This allowed for the specification of information requirements which greatly facilitated the design effort.

As is apparent from Chapters 5 and 6, virtually all of the information requirements that arose from the approach used in this effort were not captured in the previous 'status-at-a-glance' display. This result is consistent with others (e.g., Vicente & Rasmussen, 1990) and supports the use of function-based visualizations to avoid the problems that result from an over-reliance on digital presentation of raw sensor values (Woods, et al., 1991). However, at a deeper level, the point of developing a function-based visualization was to enhance cooperation between IS and human portions of a joint cognitive system. One of the key results is the potential for function-based displays to serve as a framework for the coordination and presentation of IS information otherwise hidden from the user. In the present example, IS information provided:

- additional context in which to evaluate MP behavior,
- computation and simulation of higher-order system parameters unavailable from sensor values, and
- prediction of future system state,

all of which provided enhanced visualization of changes, events, and anomalies in the MP.

Another interesting result is the interaction between efforts to develop the IS and efforts to build enhanced representational windows for the human part of the cooperative ensemble. First, information already available from the IS provided assistance in the functional modeling effort. For example, constraints on the functional relationships were an integral part of the IS's rule base. Second, the generation of information requirements provided direction for the IS model-based representation. For example, the value (in terms of the operator interface) of the simulated accumulator position was not fully realized until discussions centered on representing system integrity and inventory control.

A third result is the potential for improved communication between the human and the IS. One of the primary goals for this type of display is to make the basis on which diagnostic information from the IS is generated (symbolic computation) apparent by the behavior of the representation of the MP in the computer medium (visual computation). For example, a "blocked evaporator" message from the IS can easily be confirmed through the $\Delta t$ indication. In this manner, an experienced operator is presented with a form of concurrent graphical explanation to supplant or complement typical retrospective explanation (cf., Potter & Woods, 1991; Johns, 1990).

### 7.3.3. Integrated functional overview display development

One of the critical issues that has not been adequately addressed by previous research is the coordination of different views, as addressed by this work with respect to the complementary use of the function-based display and temporal information display to serve as an overview display. While there has been work on the importance of multiple representations in an adaptive planning context (Layton, Smith, McCoy, & Bihari, 1991), this previous work was dealing with multiple perspectives on the same process (an analogical and profile view of the flight path). Contrast this with the present

work which has focused on integrating multiple views of different processes (i.e., the MP and IS) and using information from one to enhance the representation of the other.

It is important to reconsider the work of Shafto and Remington (1990) – they found that operators did not make extensive use of the independent representation of the IS. They used it as an independent information source which they then validated through the representation of the MP. One of the goals of this work is to promote cooperative behavior of the two representations (temporal information display and function-based display).

The work of Rasmussen (1986; also Vicente & Rasmussen, 1990) supports this goal by finding that operators tend to shift perspectives (within an abstraction hierarchy framework) when trying to diagnose anomalous conditions in a complex system. This is certainly consistent with the theoretical basis for this type of decomposition in that faults tend to propagate upward in the hierarchy and reasons for normal functioning propagate downward. Thus, it is a natural mapping that an operator's perspective would need to slide up and down the hierarchy throughout diagnosis. This previous work has argued for the need to support this behavior by having the different perspectives captured by the representation and integrated in the operator interface.

The present work has focused on multiple perspectives from the approach of using one agent as a "filter" or "establishing context" for interpreting the behavior of the other. This should facilitate shifting perspectives by lessening the attentional cost involved in the shifting from one perspective to the other. The work of Kirlik (1993) is important in this regard. His results suggest that if the cost (in terms of tasks required) to engage an intelligent assistant is too high relative to the benefits (in terms of tasks offloaded), operators will tend not to enlist its service.

## 7.4. Research and design directions

### 7.4.1. On temporal issues

**How can temporal information be integrated into a function-based display?** One of the critical results of this work has been the importance of temporal information and the under-specification of it in typical representations of MP behavior. While the trend arrows used in the current 'status-at-a-glance' display are a realization of this issue, this approach falls well short of a solution.

A more specific sub-question could be *how to design real-estate-limited – information-rich trend plots*. Currently the TCS control engineers have several CRTs dedicated to the display of strip charts and several comments from the subjects indicated their reliance on these plots. However, display space limitations in the space station complex (SSC) make this approach infeasible. Thus the need arises for integrating this information into the overview display.

Figure 34 presents five approaches to address this problem. The first four are graphical annotations while the fifth is an adaptation of the 'octagon' display (Woods, Wise, & Hanes, 1981) in an attempt to convey change over time (Hansen & Skou, 1989; Jensen & Koch, 1993). This latter approach embeds several octagons, with the smaller ones depicting level in the past (analogous to depth

perception). Certainly there is a need for an empirical investigation of these (and perhaps other) approaches in order to assess their information extraction capabilities in a realistic, dynamic situation similar to TCS fault management.

A secondary sub-question is *how can we provide a mechanism for dynamically creating strip charts*. One of the results from the subject interviews was the heavy reliance on trend information, primarily in the form of strip charts. In fact, the thermal engineers prepare a list of parameters ahead of time that they are likely to want to see together on a strip chart during testing. The interface designers then define these into their interface (the interface designer's interface, not the control interface) to minimize the burden of creating these "on the fly." While the functional modeling does help specify these combinations (based on the "information requirements" in Chapter 6), there will be a need for this to be performed real-time by the controllers in the SSC as unusual or interesting situations arise.

### 7.4.2. On function-based display design

**How can functional information be integrated into physical-based displays?** As one of the recurring themes in the subject interviews was the issue that these operators focused on sensor values as their primary indication of system behavior (and were comfortable with physical schematic displays), the question arises as to how to build on this representation to concurrently provide higher-
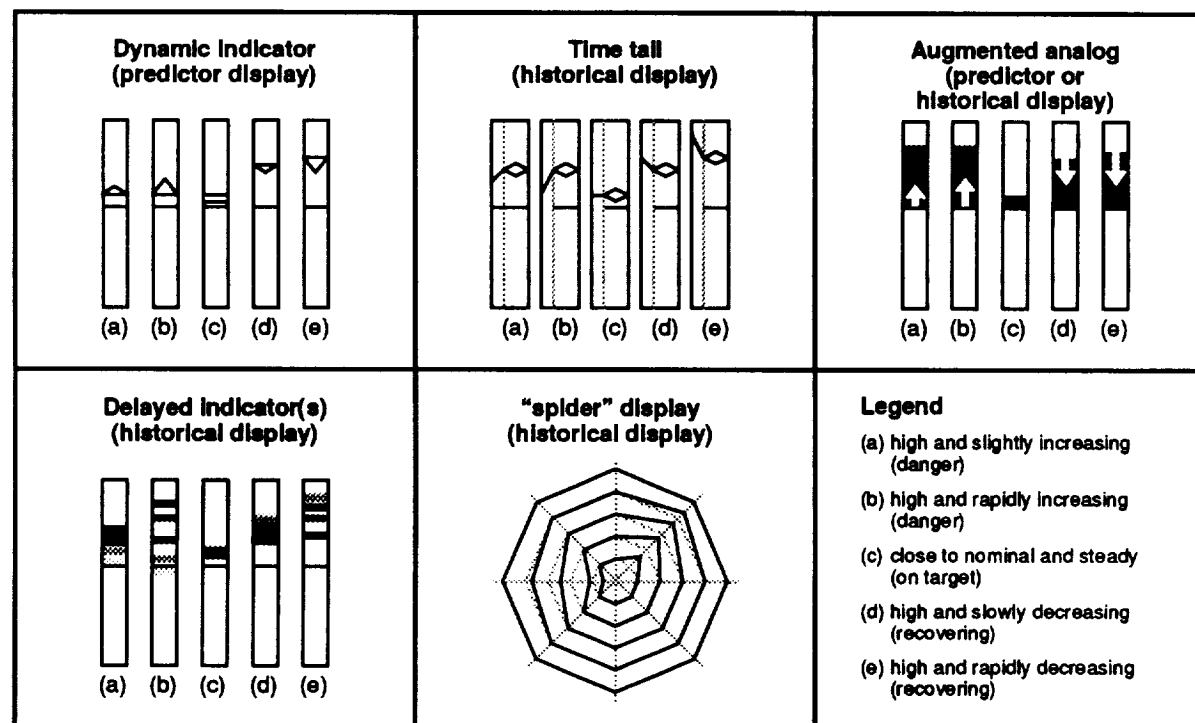


Figure 34. Alternative approaches to integrating temporal information into analog graphic formats.

level functional information. There are several possible directions to be pursued based on the underlying cause of this bias toward physical schematics.

**Criticality of representation.** One very real possibility is that enhanced representations have failed to capture the critical features of the fault management task and so operators tend to rely on what tools (representations) they have made work, despite the costs associated with using them (e.g., see the example in Section 6.3.1.8). As Section 5.6.3 discussed, the critical issue in representation design is the mapping from domain semantics (behavior of the domain) to the syntax and dynamics of the visual form. This can only be addressed by an iterative, user centered design and evaluation.

**Transfer of training.** Another possibility is that this bias comes from a transfer of training issue. The operators are experienced with particular types of displays and introducing anything new will result in a period of adjustment. Moray (1993; Moray, Jones, Rasmussen, Lee, Vicente, Brock, & Djemil, 1993) evaluated operators use of a function-based display designed for use by nuclear power plant operators compared to their traditional physical schematic displays. He found that despite preference for the traditional displays, performance was enhanced with the model (function) based display. This indicates that operators may not be able to make a priori judgments about the utility of alternative representations.

While there was not an opportunity to formally evaluate performance differences between the different versions of the two displays, it is important to distinguish *preference* and *performance* in the use of computer tools such as this. As discussed in Cook, Potter, Woods, and McDonald (1991), users' preference based on similarity to what they are comfortable with does not necessarily translate into performance advantages as well.

## 7.5. Closing thought

The fundamental issue in this work has been how to improve the communication between a monitored process, an intelligent diagnostic system, and a human operator monitoring both of these systems. Or, as the title of the sponsoring NASA grant appropriately indicated, *"Guidance for human interaction with intelligent systems: How to make AI systems team players."* It is hoped that through attention to the design of the interface between these three agents, more operators of complex systems will want an intelligent system "on their team."

# APPENDICES

# CASE STUDIES ON HUMAN INTERACTION WITH INTELLIGENT SYSTEMS

## Overview

These appendices contain case study reports for three systems – Thermal Control System, Power Management and Control, and Environmental Control and Life Support System – all NASA-sponsored advanced automation projects. These reports were written for the system developers as feedback for their efforts. Thus, they may require information not possessed by individuals unfamiliar with these systems. It is for this reason that they are included as appendices rather than integrated into the body of this report.

# Thermal Control System Advanced Automation Project

## Overview

This report is a description of work being performed as an extension of the research project on human interaction with intelligent systems that is being carried out in the Cognitive Systems Engineering Laboratory (CSEL) under a grant from NASA Johnson Space Center (*Guidelines for Human Interface with Artificial Intelligence Systems*, NAG9-390, Principal Investigator: David D. Woods).

In this project, site visits are being made to NASA-sponsored intelligent fault management system development projects in order to investigate capabilities for human interaction with intelligent systems, styles of collaboration between people and intelligent systems, and human-computer interaction (HCI) principles in these cases. The purpose of this work is twofold. First, it is designed to provide guidance to system developers on human-intelligent system interaction and HCI issues specifically related to their application in an attempt to increase awareness of the criticality of identified capabilities and functions. Second, it will expand the review of human-intelligent system interaction capabilities in aerospace intelligent fault management systems which included five NASA systems reviewed in the past year. The results will be used to support the overall project goals of identifying common themes in systems that wish to support cooperative problem solving between people and intelligent systems, to describe recurring obstacles that block effective cooperation, to point to needed capabilities, and to provide guidance to designers.

## Executive Summary

### Organization of the Report

The format of this report will revolve around three critical issues in the investigation of human-intelligent system interaction in fault management. These are (1) workspace coordination – how does the human operator navigate through the total number of displays (or views) and locate relevant data in order to monitor and control the system, (2) visualization of the state of the system (hereafter referred to as monitored process) – what capabilities are available to present the status of the monitored process (including such things as dynamic behavior and anomalies), and (3) tracking of the intelligent system activity – how are the actions and behavior of the intelligent diagnostic system represented to the operator. A summary of TCS capabilities with respect to these three issues will be

provided in the following paragraphs; more detailed descriptions will be provided in subsequent sections.

## Summary of Findings

The Schematic Browser provides adequate feedback on the displays selected and on the hierarchical structure of the different displays. The 'bus overview' selection option, which presents all three section displays (evaporator, transport, and condenser), is a mechanism based on the idea that certain arrangements of displays typically will be used in parallel and that the operator should not have to construct this arrangement from scratch each time. This is a good start on identifying these types of views, and more attention should be given to expanding on this idea.

The 'status-at-a-glance' display – while intended to function as the name implies – suffers from the same problems that plague other physical topology schematic displays. In general, this type of display is annotated with active data about the state of the monitored process (i.e., color coded digital parameter values or component states). However, this approach fails to convey the dynamic aspect of system behavior, highlight events, or indicate anomalies. Attention needs to be given to the design of status displays based on a functional model of the thermal control system.

The hierarchical structure of the schematic displays is an attempt to provide different views into the monitored process, with the impression that each view will provide unique insight not found in the others. However, the primary difference is in number of sensors presented, with considerable redundancy between displays. Additional effort needs to be devoted to an analysis of information requirements for the different levels of display.

Information from the intelligent system could possibly provide appropriate context for the operator to assess the status of the monitored process. For example, since the high fidelity simulation computes dynamic target values, these could be used to provide an "expected vs. actual" indication of system state.

## 1. Navigation Control

Navigation through the system is accomplished by the use of two features, the 'schematic browser' and display size controls on the individual displays. As is typical of most complex systems being monitored, the number of possible views far exceeds the display space on the VDU, resulting in the concern for *workspace coordination* – the coordination of the set of views into the monitored process that can be seen together in parallel or in series. At this level, the issues of concern include:

- How is the information coordinated?
- How does the user know where to look next?
- Can the user find the right data at the right time?

With this as a framework, the navigation controls for TCS will be discussed in the following paragraphs.

## Schematic Browser

This "checklist" allows for access to different views of the thermal control system and intelligent system. Multiple views can be selected to be viewed in parallel (when the display size is reduced). The format provides good feedback as to what different displays have been selected (by the use of an "x" in the box next to the display identifier) and the hierarchical organization to the displays (by the spatial organization to the checklist). More discussion will follow on the hierarchical displays. One useful feature is the 'bus overview' option which presents all three section displays (evaporator, transport, and condenser).

## Display size control

Each display contained control buttons to alter the size of the display (full, ¾, ½, and ¼). However, there are several deficiencies that were discussed:

(1) There is no feedback given as to the currently selected size.

(2) These controls appeared in different locations on different screens (i.e., lack of standardization).

Different options were discussed to work around this problem, including:

(1) Highlighting the current selection.

(2) Providing a sort of "range control" through the use of an analog display/control. This would include four selectable regions with an indication of the current selection.

(3) Differentiate these controls from the rest of the display, as they are interface controls rather than system controls.

## 2. Visualization of Monitored Process Behavior

### 'Status-at-a-glance' display

In general, this display is very similar to that used in the predecessor to TCS, HITEX. The motivation behind this type of display is in exactly the right direction. In most of the other NASA-sponsored intelligent fault management systems investigated, there was a noticeable lack of any informative displays to quickly present the overall status of the system, patterns of events, or anomalous conditions. However, in reality there are not many differences between this and other physical topology schematic displays. Therefore, the trends identified in the Woods, et al., 1991) report are applicable to the 'status-at-a-glance' display (as well as the other schematic displays). The following are more specific, relevant issues.

Trend arrows are used alongside digital values to indicate direction of change information. At this level of a display, it is certainly important to indicate trends and qualitative descriptions of system state. The arrows are obviously an indication that this need has been realized. However, while this is useful when going from steady-state to anomalous (transient) conditions, this type of display has been shown to not be useful for depicting changes within transient states. For example, a parameter that is below target level but increasing (i.e., recovering to normal) is qualitatively different than a

parameter below target level and continuing to decrease. Additional mechanisms need to be explored to efficiently present more qualitative information than just direction of change.

An issue analogous to qualitative descriptions of system state is the question of whether system goals are being met. This would include such things as exit quality from the evaporators, saturation conditions in the RFMD (as controlled by the BPRV), and accumulator level. However, there is no indication of target or goal conditions. An analysis of high-level system goals needs to be performed and this information integrated into the status display.

In other thermodynamic systems one of the critical issues is an indication of mass and energy balances within the system. It appears that similar concepts within the TCS would be the liquid/vapor balance within the RFMD, as this is the primary means by which the TCS adjusts to variations in heat load applied (and other variations in system functioning). However, this information is not presented.

One common approach is to throw away raw data, replacing it with qualitative information. However, the key is to retain this data, but provide additional information by placing it in context. An example of this is in the heat load (kW) to the evaporators. In one situation, the heat load from the two phase water heat exchanger (HX) is 1.01 kW. However, there is no indication of the range of possible values to convey qualitatively the heat load being applied. Since each cavitating venturi is adjusted to the maximum heat load for that particular evaporator, the qualitative information would allow for comparisons across different evaporators. Additionally, there is no indication of total heat load on the system to provide a summation metric.

A top-level display such as this should provide information about the context – thermal management. What operator strategies are supported (e. g., when parameter "x" is below parameter "y", do "z")? This addresses the need for a *cognitive task analysis (CTA)* of operator performance in thermal management. A CTA attempts to answer questions such as: what are the goals of the operators, how are they achieved, could they be achieved given the present conditions, and what information is required to assess system status. A critical starting point to this type of analysis is the development of *operational scenarios* to provide insight into dynamic behavior and information requirements for human operators.

One aspect of 'overview', 'quick-look', or 'status-at-a-glance' displays (by the very nature of the name) is that the system status should be readily apparent without scanning through a variety of data or performing any mental computations on the data. So, status should be the most *salient* aspect of the display (i.e., it should "pop out"). However, the most salient aspects of this display appear to be the red outline of the RFMD icon and the blue color coding of the accumulator and flow lines — both static background elements. Therefore, work also needs to focus on perceptual aspects of the interface, including color coding.

## Schematic displays

The schematic displays used in the TCS interface are designed around the physical topology of the system (and paper-based physical schematic diagrams). As such, they are very good at depicting the physical layout of the components and the interconnections between components. However, it is important to assess the purpose (or function) of these displays. Since they are annotated with system status information (in the form of raw sensor values displayed digitally), they are relied upon to provide a view of the state of the process. If they are in fact used in a monitoring role, the focus needs to be on highlighting anomalies in the TCS. However, if they are used in a diagnostic manner, they should contain the same level of detail as the paper-based schematics (which they would in essence be replacing). Given this potential dual functionality of these types of displays, there is a need for a functional analysis of the purposes that these displays will serve.

As the completeness of the schematic is increased, there is typically a simplification of detail due to limitations of real estate and legibility on a VDU. The approach used in TCS is to have a hierarchical organization. At the highest level is the status-at-a-glance display. Then, there are three "section" displays – evaporator, transport, and condenser – which provide a view into one of the three main sections of the system. At the lowest level are the 'component' displays. These views include individual evaporators and condensers, accumulators, RFMD, and BPRV. However, the additional level of detail provided by the lower level displays is very minimal. Attention needs to be given to what level of detail is appropriate for the different levels. As it stands now, the three levels can be displayed simultaneously, resulting in a proliferation of windows (Woods, et al, 1991). It would be predicted that the hierarchical structure would not be utilized, as the investment of attention to "call up" the lower level displays would be outweighed by the poor information return. In fact, research indicates that practitioners will go to great lengths to set up a pre-defined arrangement of displays and rarely vary from these within operational scenarios (Cook, Woods, McColligan, & Howie, 1990; Cook, Woods, & Howie, 1990).

## 3. Tracking Intelligent System Activity

There are two areas of focus with respect to tracking intelligent system activity. First, there is a need for the use of intelligent system information to provide additional context in which to display system status information (i.e., parameter values) typically presented on schematic displays. As a parameter can be out of tolerance based on static sensor ranges or based on dynamic, intelligent system-computed expected values (or expected trajectories), these expected values could provide additional valuable diagnostic information.

Second, attention needs to be directed toward the presentation of intelligent system reasoning and diagnosis. One of the observations from the HITEX effort was that the operators did not make extensive use of the intelligent system display; rather, they validated diagnoses by referring to the schematic display. As a result of this, it was concluded that "it is not clear whether to strive for ways to make expert system reasoning clear to operators, or to provide alternate ways for them to validate the conclusions" (Remington and Shafto, 1990).

In either case, the focus needs to be on some guiding principles for designing fault management information displays, which include:

1. *Highlight anomalies.* Since an anomaly is some departure from a reference or expected course, it is important to highlight the discrepancy.

2. *Highlight change and events.* System changes (e.g., configuration, mode, sensor availability,) and events (e.g., switch trip, heat load reduction) can provide a focus for diagnosis. Therefore, it is important to identify what are the interesting changes or sequences of behaviors.

3. *Put data in context of related values.* Typically in monitoring for anomalies it is the relationships across data values that is informative. Therefore, it is critical to collect and integrate data to build on these relationships.

## 4. Directions for future work

Based on the present discussion, there are several directions for future effort that should be pursued. First is the development of a function-based (or model-based) display to be used as a 'status-at-a-glance' display. This type of display would include functional relationships between components rather than digital display of data spatially arranged as in the physical schematic of the thermal control system. An example of some of the system goal-related information is available in the 'global parameters' display (i.e., "commanded setpoint" vs. "actual setpoint"). It is important to note that this type of display can be developed without the benefit of any integration of intelligent system information.

As the primary motivation for this project is the development of an intelligent diagnostic system, the second direction for future effort would naturally be the integration of intelligent system information into function-based displays discussed in the preceding paragraph. Since one function of the intelligent system (the high fidelity simulation in particular) is to compute dynamic target values (expected values), effort should be made to include this information into a top-level view of the status of the process. While some of this information is presented in the 'simulation overview' display, (a) it is not integrated into the current state of the process, and (b) the parameter values are not placed in context to be informative.

The temporal characteristics of the thermal management domain and the highly-coupled nature of the TCS create a need for the operator to see temporal relationships in the system (past, present, and future state) as faults propagate from the origin to other components within the system. The TCS appears to be an ideal candidate for testing concepts related to timeline displays as a means to convey temporal relationships and links between process behavior and intelligent system activity (Potter and Woods, 1991).

The fourth direction is concerned with workspace coordination. As indicated above, the hierarchical display structure allows for several views of the process to be viewed in parallel, but with

considerable redundant information in each of the displays. Attention should be given to an analysis of the amount of detail contained in each level of display.

For each of these areas, the approach to this type of display is a cognitive task analysis to identify goals and means to achieve these goals (information requirements) and the development of dynamic operational scenarios to provide a temporal evolution of incidents and real-time context for interface development and evaluation of how a human operator would interact with the information system to detect, isolate, and recover from faults within the monitored process.

# APPENDIX B

## POWER MANAGEMENT AND CONTROL SYSTEM
## ADVANCED AUTOMATION PROJECT

### Project Overview

This report is the second in a series describing work being performed as an extension of the research project on human interaction with intelligent systems that is being carried out in the Cognitive Systems Engineering Laboratory (CSEL) under a grant from NASA Johnson Space Center *(Guidelines for Human Interface with Artificial Intelligence Systems*, NAG9-390, Principal Investigator: David D. Woods).

In this project, site visits are being made to NASA-sponsored intelligent fault management system development projects in order to investigate capabilities for human interaction with intelligent systems, styles of collaboration between people and intelligent systems, and human-computer interaction (HCI) principles in these cases. The systems being investigated include:

(1) Thermal Control System (at JSC),

(2) Power Management and Control System (at LeRC), and

(3) Environmental Control and Life Support System (at MSFC).

The purpose of this work is twofold. First, it is designed to provide guidance to system developers on human-intelligent system interaction and HCI issues specifically related to their application in an attempt to increase awareness of the criticality of identified capabilities and functions. Second, it will expand the review of human-intelligent system interaction capabilities in aerospace intelligent fault management systems which included five NASA systems reviewed in the past year. The results will be used to support the overall project goals of identifying common themes in systems that wish to support cooperative problem solving between people and intelligent systems, to describe recurring obstacles that block effective cooperation, to point to needed capabilities, and to provide guidance to designers.

### 1. Introduction

During CSEL's visits to LeRC, discussions were held on three systems – Autonomous Power Expert System (APEX) for fault diagnosis, Autonomous Intelligent Power Scheduler (AIPS) to determine system configuration, and the TROUBLE fault diagnosis system. Rather than a separate report on all

106

three systems, relevant attributes of each will be discussed within the framework of a single report. To date, two visits have been made to LeRC to discuss user interface development efforts; the second occurring approximately 6 weeks after the first to discuss modifications completed (on TROUBLE) and future directions.

## Organization of the Report

The format of this report will revolve around three critical issues in the investigation of human-intelligent system interaction in fault management. These are:

- *workspace coordination* – how does the human operator navigate through the total number of displays (or views) and locate relevant data in order to monitor and control the system,

- *visualization of the state of the system* (hereafter referred to as monitored process) – what capabilities are available to present the status of the monitored process (including such things as dynamic behavior and anomalies), and

- *tracking of intelligent system activity* – how are the actions and behavior of the intelligent diagnostic system represented to the operator.

A summary of PMAC capabilities with respect to these three issues will be provided in the following paragraphs; more detailed descriptions will be provided in subsequent sections.

## Summary of Findings

One of the critical issues which needs to be addressed further in the Power Management user interface is workspace coordination. For example, in APEX, one needs to proceed to the third level of the hierarchical schematic displays before actual measured data values are presented. However, there is no indication (map) of this hierarchical display structure to guide the user through the display space. In TROUBLE, however, attempts are being made to consider what information needs to be viewed in parallel, thus providing guidance as to coordinating the different views and what information needs to be presented on the top-level schematic display.

One of the primary focus areas in our discussions on HCI (in particular with the two discussions on the TROUBLE system) has been the design of a schematic display to indicate the state of the system and related coding issues involved in the representation of system state information. Some of the issues discussed include:

- Indication of single vs. multiple anomalies,

- Indication of the state of the breakers; in particular distinguishing between an anomaly and a tripped switch,

- Voltage and current conditions of the electrical bus (which lines are energized and could deliver current if a load is applied vs. which are presently drawing current),

- Voltage margins for each of the circuits,

- Salience relationships between the various components of the schematic display (within the overall coding scheme, determining an ordinal rank-ordering of the importance of the events being depicted on the schematic and designing a coding scheme to convey this ordering).

A description of interaction capabilities to support these representations will be discussed in Section 3.

One common theme in the systems investigated in this project is the dissociation of related data. Specifically, there is a lack of integration of information from the intelligent diagnostic system and system state information. For example, the APEX system has simulation capabilities which could provide additional context for the operator to assess the state of the monitored process (i.e., expected vs. actual). This will be discussed further in Section 4.

## 2. Navigational Control

### Introduction

One of the key obstacles to effective interaction yet to be fully addressed is in the integration of information from different sources – the focus of *workspace coordination* (the coordination of the set of views into the monitored process that can be seen together in parallel or in series). At this level, the issues of concern include:

- How is the information coordinated?
- How does the user know where to look next?
- Can the user find the right data at the right time?

Previous case studies (see Woods, et al, 1991) identified a trend in similar systems in which navigational demands shift the user's focus of attention away from the monitored process and towards the interface itself. These demands are a result of placing specific types of data in separate windows without concern for what data needs to be pieced together to be informative. Therefore, a critical issue is the coordination of different views or the integration (and aggregation) of data from different views so that the operator can easily find relevant data and remain focused on monitoring and controlling the process.

### Application

Several aspects of the Power Management user interface are impacted by navigational control issues. They will be discussed in the following sections.

### Ability to view the entire hardware system

To date, only a subset of the hardware system has been included in the project. However, as the completeness of the coverage extends (i.e., as additional busses and power generation are included), attention will need to be devoted to an operator's ability to maneuver within the hardware system or ability to view the entire system at once. This is especially important since the schematic display is used (in TROUBLE in particular) as a means to provide fault detection information in addition to bus state information. Not only must the operator be able to maneuver and view the entire schematic, but the danger of an anomaly being indicated outside of the field of view must be considered.

Potential solutions to this problem include:

- Allocating more VDU real-estate to the schematic display. This would include larger VDU and/or moving to a two-monitor setup. The feasibility of this approach is being investigated by the LeRC group.

- Developing a functional display to serve as a top-level display, moving away from the reliance on physical topology schematic displays. An example of this approach is being developed for the Thermal Control System (Potter and Woods, in prep.).

- Provide an overview graphic display to serve as an alarm annunciator indicator, separating this function from the schematic display (see the discussion of visual momentum in Woods, 1984). This display would always be visible, providing a mechanism to focus operator's attention to the appropriate section of the system (that which contains the anomalous conditions).

## Integration of intelligent system and monitored process information

Much of the discussion on the TROUBLE system centered around the coordination of the intelligent system information and the related component(s) depicted on the schematic display. The problem addressed focuses on the potential for multiple anomalies detected (and thus multiple messages in the 'annunciator' window). In this situation, the operator can click on the message to obtain additional diagnostic information (in a separate Diagnostic window). However, the need was discussed for a link, or connection between related information in the three windows.

Potential approaches discussed include:

- Highlighting the component (on the schematic display) when intelligent system information is accessed, and

- Providing an identifying descriptor to the intelligent system message.

In the APEX system, diagnostic information is presented to the operator in a full-screen display without any parallel view of the current state of the power bus. Additionally, justification for the diagnosis is in another separate window. Thus, diagnostic information is presented without the context of much of the information about the current state of the power bus. To provide support for co-operative problem solving (in which the operator is actively involved in the diagnosis), capabilities need to be provided for coordinating and integrating these different types of information to prevent navigational burdens from impeding usability. One of the results from development efforts in the HITEX system (the predecessor to the Thermal Control System Automation Project) was that intelligent system diagnoses were confirmed (by the operators) by examining the current state and behavior of the system (via the process schematic) within the context of the intelligent system information (Remington and Shafto, 1990). One of the implications of this result to the Power Management system would be to provide for these types of comparisons between intelligent system messages and monitored process state.

Potential approaches include:

- Providing intelligent system activity in context of the events and changes in the electrical power system (e.g., event-driven timeline displays as in Potter and Woods, 1991), and

- Providing the ability for the two informational sources to be viewed in parallel.

## Navigating through the display space

One of the trends in workspace/navigational control is the use of "active" elements within a display which, when "clicked" reveal additional menus, displays, and/or information. The difficulty, though is the lack of feedback as to where this additional information is available. One of the design goals of the second version of TROUBLE was to differentiate between what elements were and were not "clickable." (i.e., make a button look like a button). Continuing to adhere to this principle of feedback should guide exploration of the entire workspace and provide for much greater utilization.

## Integration of the scheduling system information with the fault diagnosis system

One of the strengths of the AIPS scheduling system is the ability to view all of the activities, their temporal relationships, and resource information. This provides a "global view" of activities, with the potential to redirect the schedule if necessary (i.e., attempt to build a "better" schedule). However, APEX provides source profile data for only a given load over a period of time. It is predicted that much more scheduling information would be required by the APEX human operator.

## 3. Visualization of Monitored Process Behavior

### Introduction

In order to design an effective view of the monitored process it is imperative to define the information that the operator needs to perform his tasks (i.e., what are the information extraction goals for a particular view?) The physical schematic displays used in many of the systems reviewed are designed around the physical topology of the system (and paper-based physical schematic diagrams). As such, they are very good at depicting the physical layout of the components and the interconnections between components. For example, knowing where a sensor is located relative to other sensors/components may be important in extracting the significance of its current reading or recent behavior. If used in this type of diagnostic manner, they should contain the same level of detail as the paper-based schematics (which they would in essence be replacing). However, these same type of displays (annotated with system status information in the form of raw sensor values displayed digitally) are often used to depict the state of the monitored process, i.e., to answer questions about its overall "health". If they are in fact used in a monitoring role, the focus needs to be on highlighting anomalies in the system. Given this potential dual functionality of these types of displays, there is a need for a functional analysis of the purposes that these displays will serve.

### Application

As mentioned earlier, much of the second visit was devoted to discussions of the schematic display for TROUBLE. One of the primary reasons for this is the fact that the TAE-Plus prototyping tool is being used to develop the user interface, and modifications based on our first meeting were able to be

implemented in a short period of time. The following are some of the primary issues discussed. While these issues are directed towards TROUBLE, they are also appropriate for APEX as well.

## Single vs. multiple anomalies

Anomalies within a switch are indicated by a red square in the middle of the switch icon. However, this choice of coding does not permit indication of multiple anomalies. Potential solutions that were discussed include:

- Digital indication of the number of anomalies, and
- Coding of the icon to distinguish single vs. multiple anomalies (e.g., hue, intensity, shading).

Critical issues in choosing a coding scheme are based on questions such as:

- How many anomalies are possible? This determines the number of possible states which would have to be differentiated.
- Is the primary concern of the operator the number of anomalies or the fact that there are more than one? This question addresses the need for precise digital coding.

## Switch state information

State of the switches (off, on, tripped) are indicated by color coding of the switch icon, with the relationships being: off – dark green; on – light green; tripped – yellow. The on/off distinction is consistent with the coding of the bus to indicate voltage being provided to components. Salience issues will be discussed in a subsequent section.

## Voltage and current status

In assessing the status of the system, it is important to be able to distinguish the following states:

- Which lines are energized (have voltage)? Color coding consistent with the switch state information is used to indicate voltage.
- What loads are drawing current? When power begins to be consumed, power meters are displayed to indicate percentage of available being used.
- What loads could begin to draw current if necessary (i.e., which have voltage)? The flow path color coding also is used to indicate the presence of voltage to loads.
- Of the loads consuming power, how much reserve current is available? The power meters mentioned above indicate reserve amps. for each load.

Much useful discussion was held on coding techniques to be able to distinguish these different system states, most of which was based on some excellent ideas generated by the LeRC group in the interim between CSEL visits.

## Salience relationships

One problem discussed is the interaction between anomaly and switch state indications. The yellow (tripped) state is much more salient than the anomaly (red) depiction. This is due to the joint effect of size and intensity, both causing a large yellow region to be more salient than a small red one.

Additional coding techniques are being explored to work around this problem. One of the interesting issues raised in this context is the role of guidelines (such as the *Baseline Space Station Freedom Program (SSFP) Flight Human-Computer Interface Standards* – NASA, 1991). This document imposed standard icons for different components in the schematic display which limited the choice of coding techniques to indicate switch state.

One of the critical steps in determining salience relationships is the development of a salience table that relates events and components to be coded to the selection of available coding techniques. For example, different switch states are identified and related (in terms of desired salience) to each other as well as to the other items in the interface. Then, after all of the elements are identified and rank-ordered, coding selections are made from available techniques (e.g., size, intensity, shape, hue, spatial grouping, dynamic behavior, etc.).

A key element of this approach is that it provides an organizational structure to the coding process and emphasizes the *interactions* among the different coding selections. Using such a systematic approach identifies any overuse of a single coding mechanism (most typically hue) and points to alternate means of highlighting change and events in the monitored process.

## 4. Tracking Intelligent System Activity

### Introduction

Another of the findings of the previous case studies of NASA-sponsored intelligent system development effort was the lack of attention given to the output from the intelligent system. To integrate human and machine problem solvers into an effective cooperative system, the intelligent system output needs to be structured in a manner that supports operator visualization of critical events and intelligent system's assessment, diagnoses, and recommended actions in response to these events. Typically, this information is presented in the form of chronologically ordered message lists. However, this form does not capture any of the temporal information that is necessary for the event-driven nature of the fault management task and it does not provide any context in which to interpret the diagnoses.

### Application

There are two areas of focus with respect to tracking intelligent system activity. In each case the key is on using one source of information as context to assist the operator in interpreting another source. First, there is a need for the use of intelligent system information to provide additional context in which to display system status information (i.e., parameter values) typically presented on schematic displays. As a parameter can be out of tolerance based on static sensor ranges *or* based on dynamic, intelligent system-computed expected values, these expected values could provide additional valuable diagnostic information. While this approach was only briefly discussed in the context of the Power Management project, it should be pursued further as a means of highlighting discrepancies in parameter values.

Second, attention needs to be directed toward the presentation of intelligent system reasoning and diagnosis in the context of the events and status of the monitored process. Traditional means of displaying intelligent system activity have not proven to be effective in similar applications (Remington and Shafto, 1990). There is a need to support validation of diagnoses through comparisons of the intelligent system's assessment of process state vs. those of the operator based on information from the view into the state of the system.

The design principle for this approach is that intelligent system information should be linked to the events and change in the monitored process (Potter & Woods, 1991). This is a concept that received some discussion within the TROUBLE project and is critical to the integration of information and the human operator's ability to understand what is happening in the monitored process and how the intelligent system is responding to events. It is important to put data in context of related information to indicate relationships. Since the intelligent system is responding to changes in the monitored process, these events and changes are the appropriate context in which diagnoses and recommendations need to be presented.

## 5. Discussion and Future Directions

Several principles for designing information displays are appropriate to the obstacles encountered in the Power Management project:

In designing information displays, it is generally useful to retain quantitative information (raw data), but supplement it with qualitative information (to provide context in which to interpret the raw data). This is demonstrated very nicely in TROUBLE in which the current-set-point (amps) and current-in-line (also in amps) are annotated on the schematic display. However, there are also the adaptive power meters to provide a qualitative view of current margin. Contrast this with the APEX system in which raw data is only presented on a schematic display three layers deep in the interface structure. This approach leads to a proliferation of windows (Woods, et al, 1991).

In the design of top-level 'overview' displays, system status should be readily apparent without scanning through a variety of data or performing any mental computations on the data. So, status should be the most *salient* aspect of the display (i.e., it should "pop out"). This point has received attention in the TROUBLE interface based on our first meeting. Static elements of the display that in themselves do not carry status information have been eliminated and system behavior is conveyed through dynamic icons and coding techniques.

One of the critical design goals is to highlight change and events. System changes (e.g., configuration, mode, sensor availability,) and events (e.g., switch trip, load modifications) can provide a focus for diagnosis. Therefore, it is important to identify what are the interesting changes or sequences of behaviors. This leads to the need for development of *operational scenarios* in which to evaluate potential designs. These scenarios should provide insights into dynamic behavior and information requirements for human operators by defining the temporal evolution of incidents in a real-time context. In the power management domain, the temporal structure of events appears to be much

shorter than that of the thermal or environmental control systems. However, there certainly is flexibility in potential configurations of the power bus that could provide a framework for scenario development.

# APPENDIX C

# ENVIRONMENTAL CONTROL AND LIFE SUPPORT SYSTEM ADVANCED AUTOMATION PROJECT

## Project Overview

This report is the third in a series describing work being performed as an extension of the research project on human interaction with intelligent systems that is being carried out in the Cognitive Systems Engineering Laboratory (CSEL) under a grant from NASA Johnson Space Center *(Guidelines for Human Interface with Artificial Intelligence Systems,* NAG9-390, Principal Investigator: David D. Woods).

In this project, site visits have been made to NASA-sponsored intelligent fault management system development projects in order to investigate capabilities for human interaction with intelligent systems, styles of collaboration between people and intelligent systems, and human-computer interaction (HCI) principles in these cases. The systems being investigated include:

(1) Thermal Control System (at JSC),

(2) Power Management and Control System (at LeRC), and

(3) Environmental Control and Life Support System (at MSFC).

The purpose of this work is twofold. First, it is designed to provide guidance to system developers on human-intelligent system interaction and HCI issues specifically related to their application in an attempt to increase awareness of the criticality of identified capabilities and functions. Second, it will expand the review of human-intelligent system interaction capabilities in aerospace intelligent fault management systems which included five NASA systems reviewed in the past year. The results will be used to support the overall project goals of identifying common themes in systems that wish to support cooperative problem solving between people and intelligent systems, to describe recurring obstacles that block effective cooperation, to point to needed capabilities, and to provide guidance to designers.

## 1. Introduction

At the date of the visit by CSEL, little attention had been given to an end-user interface for ECLSS. Rather, the interface was oriented towards system developers. As such, many of the HCI issues had not been addressed and may be planned on being implemented within a user interface. The focus of

115

this report, then, is to provide prescriptive assistance (rather than the more reactionary type of guidance in the other reports) in hopes of avoiding the typical problems encountered in the other systems studied. In general, the interface features presently contained in ECLSS are very similar to the other KATE applications at KSC (most notably the Environmental Control System). Since KATE was included in the earlier set of case studies performed by CSEL, the interested reader is referred to Woods, et al. (1991a, b).

## Organization of the Report

The format of this report will revolve around three critical issues in the investigation of human-intelligent system interaction in fault management. These are:

- *workspace coordination* – how does the human operator navigate through the total number of displays (or views) and locate relevant data in order to monitor and control the system,

- *visualization of the state of the system* (hereafter referred to as monitored process) – what capabilities are available to present the status of the monitored process (including such things as dynamic behavior and anomalies), and

- *tracking of intelligent system activity* – how are the actions and behavior of the intelligent diagnostic system represented to the operator.

## Summary of Findings

One of the critical issues which will need to be addressed in the ECLSS interface development effort is workspace coordination. For example, in the 'overview' display, parameter values are accessed by clicking on the relevant component and selecting from a menu. This type of interaction would impose interface burdens and prohibit any comparisons across parameters (a typical activity when assessing monitored process status). In addition, when the entire ECLSS system is included (rather than just the Carbon Dioxide Removal Assembly (CDRA) subsystem) there will be navigation difficulties in moving through the entire system.

A second critical issue is the need to support an operator's understanding of the state of the system and the intelligent system's response to changes and events. An overview display such as presently implemented is similar to those in the other systems, lacking goal-related information (is the system achieving its goal?) and failing to highlight events and dynamic behavior. One of the results of the testbed operations for the Thermal Control System was the lack of informativeness of the 'status-at-a-glance' overview display and its subsequent lack of utility. As issues relevant to the development of a user interface are addressed by the ECLSS project, of highest importance will be the development of interaction capabilities to permit the operator to easily visualize the events and activities of the monitored process and intelligent system.

## 2. Navigational Control

### Introduction

One of the key obstacles to effective interaction is the integration of information from different sources – the focus of *workspace coordination* (the coordination of the set of views into the monitored process that can be seen together in parallel or in series). At this level, the issues of concern include:

- How is the information coordinated?
- How does the user know where to look next?
- Can the user find the right data at the right time?

Previous case studies (see Woods, et al., 1991a) identified a trend in similar systems in which navigational demands shift the user's focus of attention away from the monitored process and towards the interface itself. These demands are a result of placing specific types of data in separate windows without concern for what data needs to be pieced together to be informative. Therefore, a critical issue is the coordination of different views or the integration (and aggregation) of data from different views so that the operator can easily find relevant data and remain focused on monitoring and controlling the process.

### Application

Several aspects of the ECLSS interface are impacted by navigational control issues. They will be discussed in the following sections.

#### Ability to view the entire hardware system

To date, only a subset of the ECLSS hardware system has been included in the project, as the model-based reasoning effort has been focused on the CDRA. However, as the completeness of the coverage extends (i.e., as additional subsystems are included), attention will need to be devoted to an operator's ability to maneuver within the hardware system or ability to view the entire system at once. This is especially important since (in the other systems studied) schematic displays are used as a means to provide fault detection information in addition to system state information. Not only must the operator be able to maneuver and view the entire schematic, but the danger of an anomaly being indicated outside of the field of view must be considered.

#### Integration of intelligent system and monitored process information

In the present configuration, intelligent system information is presented in the 'diagnoser' and 'messages' windows, which (it is assumed) are each full-screen windows. Thus, diagnostic information is presented without the context of information about the current state of the monitored process. To provide support for cooperative problem solving (in which the operator is actively involved in the diagnosis), capabilities need to be provided for coordinating and integrating these different types of information to prevent navigational burdens from impeding usability. One of the

results from development efforts in the HITEX system (the predecessor to the Thermal Control System Automation Project) was that intelligent system diagnoses were confirmed (by the operators) by examining the current state and behavior of the system (via the process schematic) within the context of the intelligent system information (Remington and Shafto, 1990). One of the implications of this result to ECLSS would be to provide for these types of comparisons between intelligent system messages and monitored process state. Potential solutions include providing intelligent system activity in context of the events and changes in ECLSS (e.g., event-driven timeline displays as in Potter & Woods, 1991), and providing capabilities to view the two informational sources in parallel.

### Navigating through the display space

One of the features of the 'overview' display in terms of workspace/navigational control is the use of "active" elements which, when clicked via the mouse, reveal a menu containing options of viewing frame representations, hierarchical relationships, parameter values, and various other operations. One difficulty, though, is the lack of feedback as to where this additional information is available. Norman (1988) discusses the importance of feedback in inviting exploration of the system. Cook, et al. (1990 a, b) found that practitioners set up pre-defined arrangements of displays and rarely vary from these configurations within operational scenarios. Most of the user-selectable options in these studies went unexplored.

One of the design goals of the user interface to the Power Management system (after the initial CSEL visit) was to differentiate between what elements were and were not "clickable." (i.e., differentiate between controls and displays). Continuing to adhere to this principle of feedback should guide exploration of the entire workspace and provide much greater utilization.

## 3. Visualization of Monitored Process Behavior

### Introduction

In order to design an effective view of the monitored process it is imperative to define the information that the operator needs to perform his tasks (i.e., what are the information extraction goals for a particular view?) The physical schematic displays used in many of the systems reviewed are designed around the physical topology of the system (and paper-based physical schematic diagrams). As such, they are very good at depicting the physical layout of the components and the interconnections between components. For example, knowing where a sensor is located relative to other sensors/components may be important in extracting the significance of its current reading or recent behavior. If used in this type of diagnostic manner, they should contain the same level of detail as the paper-based schematics (which they would in essence be replacing). However, these same type of displays (annotated with system status information in the form of raw sensor values displayed digitally) are often used to depict the state of the monitored process, i.e., to answer questions about its overall "health". If they are in fact used in a monitoring role, the focus needs to be on highlighting anomalies in the system.

## *Application*

Since a schematic display has not been developed for ECLSS, this section will discuss relevant issues and use examples from the other NASA/Code MT systems as illustrations. The similarity between the systems should lend to generalizability of the issues.

### Target conditions

A key element of a view into the monitored process is an indication of whether system goals are being met. This would include such things as the top-level functional purposes of the system. In the water recovery system within ECLSS, this would be temperature conditions in the second reservoir (is the water hot enough to kill bacteria?). Within the CDRA, goals would include relative humidity of the air (as it is dehumidified and later rehumidified), temperature (as it is cooled), and $CO_2$ concentrations (since the primary purpose of the system is to remove $CO_2$). One of the main deficiencies of many schematic displays is the failure to provide an indication of target (goal) vs. actual conditions. A functional analysis of high-level system goals needs to be performed and this information integrated into a top-level status display (see Vicente & Rasmussen, 1990; Potter & Woods, 1992).

### Trends

A key aspect of dynamic systems is their ability to change and evolve over time. In monitoring for changes in the system, it is important to have information about trends in the data (qualitative descriptions of system state) to be able to assess system health and predict future state. The 'status-at-a-glance' display for the Thermal Control System attempts to achieve this goal by including trend arrows alongside digital parameter values. However, while this is useful when going from steady-state to anomalous (transient) conditions, this type of display has been shown to not be useful for depicting changes within transient states. For example, a parameter that is below target level but increasing (i.e., recovering to normal) is qualitatively different than a parameter below target level and continuing to decrease (i.e., deteriorating). Additional mechanisms need to be explored to efficiently present more qualitative information than just direction of change.

### Providing data in context

One approach in designing top-level status displays is to throw away raw data, replacing it with qualitative information. However, the key is to retain this quantitative data, but provide additional information by placing it in context. An example of this is in the heat load (in kW) being applied to the evaporators in the Thermal Control System. In one situation, the heat load from one heat exchanger is 1.01 kW. However, in the status-at-a-glance display there is no indication of the range of possible values to convey qualitatively the heat load being applied. Such a qualitative information would allow for comparisons across different evaporators. Additionally, there is no indication of total heat load on the system to provide a summation metric. A solution to this problem is not to present only a qualitative coding of the data, but to provide both quantitative data and qualitative description in combination.

## Single vs. multiple anomalies

A typical mechanism for indicating anomalous conditions is color coding of the affected component(s). One of the problems of this approach is the inability to indicate whether:

- one fault is causing several anomalous conditions or multiple faults are present,
- a component contains multiple faults.

As part of the discussion on the Power Management project, discussion was held on potential solutions, including:

- digital indication of the number of anomalies, and
- coding of the icon to distinguish single vs. multiple anomalies.

Critical issues in choosing a coding scheme are based on questions such as:

- How many anomalies are possible (within a given component)? This determines the number of possible states which would have to be differentiated.
- Is the primary concern of the operator the number of anomalies or the fact that there are more than one? This question addresses the need for precise digital coding.

## Hierarchical schematic display structure

As the completeness of the schematic is increased (in terms of amount of the monitored process depicted), there is typically a simplification of detail due to limitations of real estate and legibility on a VDU. The approach used in the Thermal Control System is to have a hierarchical organization of schematic displays. At the highest level is the 'status-at-a-glance' display. Then, there are three 'section' displays – evaporator, transport, and condenser – which provide a view into one of the three main sections of the system. At the lowest level are the 'component' displays. These views include individual evaporators and condensers, accumulators, RFMD, and BPRV. However, the additional level of detail provided by the lower level displays is primarily the addition of some sensor values. In designing this type of representation, attention needs to be given to what level of detail is appropriate for the different levels. Based on CSEL's visit to TCS, it was predicted that the hierarchical structure would not be utilized, as the investment of attention to "call up" the lower level displays would be outweighed by the poor information return. In fact, during test-bed operations, the middle-level displays were rarely used.

## Salience relationships

One aspect of overview displays (by the very nature of the name) is that the system status should be readily apparent without scanning through a variety of data, performing any mental computations on the data, or searching for relevant data in other parts of the display space. So, status should be the most *salient* aspect of the display (i.e., it should "pop out"). This point was discussed during CSEL's visit to ECLSS based on ongoing work with the other Code MT projects. Static elements of the display that in themselves do not carry status information should be eliminated and system behavior conveyed through dynamic behavior of the interface. The current 'overview' display for ECLSS, is

only a map of the system. All information has to be accessed through interface mechanisms (via clicking on active elements in the display). As the ECLSS user interface is developed, considerable attention needs to be focused on this aspect of the interface.

One of the critical steps in determining salience relationships is the development of a salience table that relates events and components to be coded to the selection of available coding techniques. For example, different switch states are identified and related (in terms of desired salience) to each other as well as to the other items in the interface. Then, after all of the elements are identified and rank-ordered, coding selections are made from available techniques (e.g., size, intensity, shape, hue, spatial grouping, dynamic behavior, etc.).

A key element of this approach is that it provides an organizational structure to the coding process and emphasizes the *interactions* among the different coding selections. Using such a systematic approach identifies any overuse of a single coding mechanism (most typically hue) and points to alternate means of highlighting change and events in the monitored process.

## 4. Tracking Intelligent System Activity

### Introduction

Another of the findings of the previous case studies of NASA-sponsored intelligent system development effort was the lack of attention given to the output from the intelligent system. To integrate human and machine problem solvers into an effective cooperative system, the intelligent system output needs to be structured in a manner that supports an operator's visualization of critical events in the monitored process and intelligent system's assessment, diagnoses, and recommended actions in response to these events. Typically, this information is presented in the form of chronologically ordered message lists. However, this form does not capture any of the temporal information that is necessary for the event-driven nature of the fault management task and it does not provide any context in which to interpret the diagnoses.

### Application

There are two areas of focus with respect to tracking intelligent system activity. In each case the key is on using one source of information as context to assist the operator in interpreting another source. First, there is a need for the use of intelligent system information to provide additional context in which to display system status information (i.e., parameter values) typically presented on schematic displays. As a parameter can be out of tolerance based on static sensor ranges *or* based on dynamic, intelligent system-computed expected values, these expected values could provide additional valuable diagnostic information. While this approach was only briefly discussed in the context of the ECLSS project, it should be pursued further as a means of highlighting discrepancies in parameter values.

The diagnosis algorithm used in ECLSS (KATE) scans a set of observed measurements and compares them to a set of simulated values (obtained by propagating commands forward through a

network of component models) to detect faults. Once a measurement is found to be discrepant, the diagnoser is invoked to localize the fault to the extent possible. Therefore, faults are considered to be differences between expected (simulated) and actual values. In addition to the diagnostic advantages of this approach, there can also be potential advantages of this technique as a useful tool with respect to HCI issues. It may be extremely useful to indicate this expected/actual difference in a situation in which a parameter is high (based on typical operational range) but normal (based on simulated value from KATE). Thus, the simulated value provides operational-specific context in which to evaluate the current sensor reading.

One cautionary note, though, is that this approach depends on the validity of the model. An invalid or untuned model can cause the constant invocation of the diagnoser, even when there is no fault in the monitored process (i.e., present "false alarms"). As mentioned in the Boeing ECLSS Advanced Automation Project 1991 Annual Report:

> ". . . the ECLSS is a set of highly interdependent subsystems, whose interaction has been isolated to a set of well-controlled water and gas buffers. these interactions (and the operations of the system as a whole) cannot easily be expressed in engineering terms given the atmospheric, chemical, and biological processes defined across the multiple interfaces." (Boeing, 1991; p. 6).

This type of complexity is also present in the other NASA/Code MT projects, as is evident from Hill and Faltisco (1991):

> "Both of these components [referring to the Back Pressure Regulator Valve and the Rotary Fluid Management Device within the Thermal Control System] exhibit highly nonlinear nominal behavior which makes constructing dynamic numerical simulations difficult." (Hill & Faltisco, 1991; p. 983).

This implies the need to provide mechanisms for the operator's ability to validate the model based on his/her internal knowledge and a view of the status of the monitored process.

Second, attention needs to be directed toward the presentation of intelligent system reasoning and diagnosis in the context of the events and status of the monitored process. Traditional means of displaying intelligent system activity have not proven to be effective in similar applications (Remington & Shafto, 1990). There is a need to support validation of diagnoses through comparisons of the intelligent system's assessment of process state vs. those of the operator based on information from the view into the state of the system.

The design principle for this approach is that intelligent system information should be linked to the events and change in the monitored process (Potter & Woods, 1991). This is a concept that arose from previous case studies and is critical to the integration of information and the human operator's ability to understand what is happening in the monitored process and how the intelligent system is responding to events. It is important to put data in context of related information to indicate relationships. Since the intelligent system is responding to changes in the monitored process, these events and changes are the appropriate context in which diagnoses and recommendations need to be presented.

# 5. Discussion and Future Directions

As this report has attempted to emphasize, one of the key aspects of human-intelligent system interaction in environments such as ECLSS is the operator's ability to visualize the state of the system through the representation conveyed by the computer medium (Woods, 1991). Along these lines, the question to be addressed in the interface development effort is what capabilities should be available to present the status of the monitored process – including such things as dynamic behavior and anomalies – in a manner that will support human problem solving about the cause(s) of the anomalous behavior. While the development of intelligent systems (such as these studied) can potentially provide extremely powerful capabilities for fault detection, isolation, and recovery (FDIR), they typically hide what they know about system state, activity, and goals from the human agents in the cooperative ensemble. In this manner, the intelligent system provides another source of data and serves to exacerbate the problem of data overload (cf., Potter & Woods, 1991) for the human operator who is already facing a cognitively demanding task of trying to ascertain system status based on raw telemetry data.

Two research directions are being pursued by CSEL within this JSC project which should be emphasized in advanced automation projects such as ECLSS. First is the development of a function-based (or model-based) display that will work as an assessment vehicle for human monitors. This type of display includes functional relationships between components rather than digital display of data spatially arranged. The support system is based on Rasmussen's (1986) and similar conceptual frameworks for describing the human operator's cognitive task. As the primary motivation for this project is the development of an intelligent diagnostic system, the second focus needs to be (as discussed in Section 4) on the integration of intelligent system information into function-based displays. Using a function-based view as a framework to coordinate intelligent system information results in a prescriptive approach to the specification of information requirements from that same intelligent system (Mitchell & Saisi, 1987).

As a critical design goal in interface development efforts for process control environments is to highlight change and events, system changes (e.g., configuration, mode, sensor availability,) and events (e.g., switch trip, load modifications) can provide a focus for diagnosis. Therefore, it is important to identify what are the interesting changes or sequences of behaviors. This leads to the need for development of *operational scenarios* in which to evaluate potential designs. These scenarios should provide insights into dynamic behavior and information requirements for human operators by defining the temporal evolution of incidents in a real-time context. One of the critical features of these types of scenarios is the temporal nature of the domain. For example, the temporal structure of events within the power management domain appears to be much shorter than that of the thermal or environmental control systems. The utility of these operational scenarios increases as the temporal dimension and the flexibility in potential configurations of the monitored process expand (the latter of which could provide a framework for scenario development), and the development of these scenarios is critical for evaluating HCI capabilities.

# BIBLIOGRAPHY

Abbott, K. H. (1988). Robust operative diagnosis as problem solving in a hypothesis space. In *Proceedings of the Seventh National Conference on Artificial Intelligence*, American Association for Artificial Intelligence.

Abbott, K. H. (1990). Robust fault diagnosis of physical systems in operation. PhD. Dissertation. New Brunswick, NJ: Rutgers University.

Abbott, T. S. (1989). Task-oriented display design: Concept and example. *SAE Technical Paper Series #892230*. Aerospace Technology Conference and Exposition. Sept. 25-28, 1989. Anaheim, CA: SAE.

Abbott, T. S. (1990). A simulation evaluation of the engine monitoring and control system display. *NASA Technical Paper #2960*. Hampton, VA: NASA Langley Research Center.

Adelman, L., Cohen, M. S., Bresnick, T. A., Chinnis, J. O. Jr., and Laskey, K. B. (1992). Real-time expert system interfaces, cognitive processes, and task performance: An empirical assessment. *Human Factors, 35*(2). pp. 243-261.

Allen, J. F. (1984). Towards a general theory of action and time. *Artificial Intelligence, 23*. pp. 123-154.

Alty, J. L. and Coombs, M. J. (1980). Face-to-face guidance of university computer users – I: A study of advisory services. *International Journal of Man-Machine Studies, 12*, pp. 390-406.

Beltracchi, L. (1989). Energy, mass, model-based displays, and memory recall. *IEEE Transactions on Nuclear Science, 36*, June, 1989. pp. 1367-1381.

Bennett, K. B. (1991). Representational aiding for a complex, dynamic control task. In *Proceedings of the 1991 IEEE International Conference on Systems, Man, and Cybernetics*. Charlottesville, VA: IEEE. pp. 1207-1212.

Bennett, K. B. and Flach, J. M. (1992). Graphical displays: Implications for divided attention, focused attention, and problem solving. *Human Factors, 34*(5), pp. 513-534.

Bennett, K. B., Toms, M. L., and Woods, D. D. (1993). Emergent features and graphical elements: Designing more effective configural displays. *Human Factors, 35*(1), pp. 71-97.

Boeing Computer Services (December, 1991). Environmental Control and Life Support System Advanced Automation Project – 1991 Annual Report. Huntsville, AL: Boeing.

Boff, K. and Lincoln, J. (1988). *Engineering data compendium*. Wright Patterson AFB, OH: Harry Armstrong Aerospace Medical Research Laboratory.

Clausewitz, C. Von (1968). *On War*, ed. Anatol Rapoport. Harmondsworth: Pelican.

Cook, R. I., Woods, D. D., McColligan, E., and Howie, M. B. (1990a). Cognitive consequences of "clumsy" automation on high workload, high consequence human performance. In *Space Operations, Applications and Research Symposium (SOAR '90)*. Houston, TX: NASA Johnson Space Center.

Cook, R. I., Woods, D. D., and Howie, M. B. (1990b). The natural history of introducing new information technology into a dynamic high-risk environment. In *Proceedings of the Human Factors Society 34th Annual Meeting*, Santa Monica, CA: The Human Factors Society.

Cook, R. I., Potter, S. S., Woods, D. D., and McDonald, J. S. (1991). Evaluating the human engineering of microprocessor-controlled operating room devices. *Journal of Clinical Monitoring, 7*, pp. 217-226.

Coombs, M. J. and Alty, J. L. (1980). Face-to-face guidance of university computer users --II: Characterizing advisory interactions. *International Journal of Man-Machine Studies, 12*, pp. 407--429.

Coombs, M. J. and Alty, J. L. (1984). Expert systems: An alternative paradigm. *International Journal of Man-Machine Studies, 20*, pp. 21-43.

Czerwinski, M. P. (1991). Automated system function allocation and display format. Submitted for publication.

Decortis, F., De Keyser, V., Cacciabue, P. C., and Volta, G. (1991). The temporal dimension of man-machine interaction. In G. R. S. Weir and J. L. Alty (Eds.) *Human-Computer Interaction and Complex Systems*, London: Academic Press.

Fischer, G. (1989). Human-computer interaction software: Lessons learned, challenges ahead. *IEEE Software*, pp. 44-52.

Goodstein, L. P. and Rasmussen, J. (1988). Representation of process state, structure,and control. *Le Travail Humain, 51*, pp. 19-37.

Hansen, J. P. and Skou, C. V. (1989). Time tunnels – an ecological interface for dynamic data. Risø National Laboratory Technical Report. Roskilde, Denmark.

Hill, T. and Faltisco, R. M. (March, 1991). Intelligent fault management for the space station active thermal control system. In *Fifth Annual Workshop on Space Operations, Applications, and Research (SOAR '91)*, NASA Conference Publication-3127 Vol. 1, Houston, TX: NASA Johnson Space Center.

Hollnagel, E. (1992). The intelligent use of intelligent systems. In *NATO Advanced Research Workshop on Intelligent Systems: Safety, Reliability and Maintainability Issues*. August 24-27, 1992. Kusadasi, Turkey.

Jensen, L. P. and Koch, P. (1993). An ecological man-machine interface for temporal visualization. In W. D. Gray, W. E. Hefley, and D. Murray (Eds.), *Proceedings of the 1993 International Workshop on Intelligent User Interfaces.* Orlando, Fl. New York: ACM Press. pp. 235-238.

Johns, G. L. (1990). Graphical interfaces to intelligent fault management systems: Issues and guidelines. MITRE Report # MTR-90W00103. Houston, TX: NASA.

Jones, P. M., Wickens, C. D., and Deutch, S. J. (1990). The display of multivariate information: An experimental study of an information integration task. *Human Performance, 3*(1), pp. 1-17.

Kirlik, A. (1993). Modeling strategic behavior in human-automation interaction: Why an "aid" can (and should) go unused. *Human Factors, 35*(2), pp. 221-242.

Kolcum, E. H. (1992). Lockheed expert system to allow real-time evaluation of shuttle fueling. *Aviation Week and Space Technology.* May 11, 1992. p. 57.

Layton, C. F., Smith, P. J., McCoy, C. E., and Bihari, T. (1991). Multiple representations for adaptive planning: Concepts and benefits. In *Proceedings of the 1991 IEEE International Conference on Systems, Man, and Cybernetics.* Charlottesville, VA: IEEE. pp. 1201-1205.

Lind, M. (1991). Representations and abstractions for interface design using multilevel flow modelling. In G. R. S. Weir and J. L. Alty (Eds.), *Human-Computer Interaction and Complex Systems.* London: Academic Press.

Lupton, L. R., Lapointe, P. A., and Guo, K. Q. (1992). Survey of international developments in alarm processing and presentation techniques. In *1992 IAEA International Conference on Nuclear Power Plant Instrumentation and Control.* May, 1992. Tokyo, Japan.

Malin, J. T., Schreckenghost, D. L., Woods, D. D., Potter, S. S., Johannesen, L., Holloway, M., and Forbus, K. D. (September, 1991a). Making intelligent systems team players: Case studies and design issues. Volume I: Human-computer interaction design. *NASA Technical Memorandum 104738.* Houston, TX: NASA Johnson Space Center.

Malin, J. T., Schreckenghost, D. L., Woods, D. D., Potter, S. S., Johannesen, L., Holloway, M., and Forbus, K. D. (September, 1991b). Making intelligent systems team players: Case studies and design issues. Volume II: Fault management system cases. *NASA Technical Memorandum 104738.* Houston, TX: NASA Johnson Space Center.

McCormick, E. J and Sanders, M. S. (1987). *Human factors engineering and design.* New York: McGraw-Hill.

Mitchell, C. and Saisi, D. (1987). Use of model-based qualitative icons and adaptive windows in workstations for supervisory control systems. *IEEE Transactions on Systems, Man, and Cybernetics, SMC-17,* pp. 573--593.

Moray, N. (1993). Direct perception interfaces for nuclear power plants. In *Cognitive Science Approaches to Process Control '93.* Copenhagen.

Moray, N., Jones, B. J., Rasmussen, J., Lee, J. D., Vicente, K. J., Brock, R., and Djemil, T. (1993). A performance indicator of the effectiveness of human-machine interfaces for nuclear power plants. USNRC Technical Report NUREG/CR-5977. Washington, DC: U.S. Nuclear Regulatory Commission.

NASA (October, 1991). Baseline Space Station Freedom Program (SSFP) Flight Human-Computer Interface Standards. SSP 30570.

Norman, D. A. (1988). *The psychology of everyday things.* New York: Basic Books. Also published in paperback as Norman, D. A. (1990). *The design of everyday things.* New York: Doubleday.

O'Hara, J. and Brown, W. (1991). Nuclear power plant alarm systems: Problems and issues. In *Proceedings of the Human Factors Society 35th Annual Meeting,* Santa Monica, CA: The Human Factors Society. pp. 1233-1237.

Potter, S. S. and Woods, D. D. (1991). Event driven timeline displays: Beyond message lists in human-intelligent system interaction. In *Proceedings of the 1991 IEEE International Conference on Systems, Man, and Cybernetics.* Charlottesville, VA: IEEE.

Potter, S. S. and Woods, D. D. (1992a). Case studies on human interaction with intelligent systems: Environmental control and life support system advanced automation project. CSEL Technical Report. Columbus, OH: The Ohio State University.

Potter, S. S. and Woods, D. D. (1992b). Case studies on human interaction with intelligent systems: Power management and control system advanced automation project. CSEL Technical Report. Columbus, OH: The Ohio State University.

Potter, S. S. and Woods, D. D. (1992c). Case studies on human interaction with intelligent systems: Thermal control system advanced automation project. CSEL Technical Report. Columbus, OH: The Ohio State University.

Potter, S. S., Woods, D. D., Hill, T., Boyer, R. L., and Morris, W. S. (Oct., 1992). Visualization of dynamic processes: Function-based displays for human-intelligent system interaction. In *Proceedings of the 1992 IEEE International Conference on Systems, Man, and Cybernetics.* Chicago, IL: IEEE. pp. 1504-1509.

Quinn, T. M. and Walters, J. L. (1991). An autonomous fault detection, isolation, and recovery system for a 20-kHz electric power distribution test bed. NASA Technical Memorandum 104344. Cleveland, OH: NASA Lewis Research Center.

Rasmussen, J. (1986). *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering.* New York: North-Holland.

Remington, R. W. and Shafto, M. G. (1990). Building human interfaces to fault diagnostic expert systems I: Designing the human interface to support cooperative fault diagnosis. In *CHI'90 Workshop on Computer-Human Interaction in Aerospace Systems.* Seattle, WA. April 1-2, 1990.

Ringer, M. J. (1991). Autonomous power system: Integrated scheduling. In *1991 Space Operations, Applications, and Research Symposium*. Houston, TX.

Roberts, K. H., and Rousseau, D. M. (1989). Research in nearly failure-free, high reliability systems: "Having the bubble." *IEEE Transactions, 36*. pp. 132-139.

Robertson, S. P., Zachary, W., and Black, J. (1990). (Eds.) *Cognition, Computing and Cooperation*, New Jersey: Ablex.

Roth, E. M., Bennett, K., and Woods, D. D. (1987). Human interaction with an "intelligent" machine. *International Journal of Man-Machine Studies, 27*, pp. 479--525

Roth, E. M. and Woods, D. D. (1988). Aiding human performance: I. Cognitive analysis. *Le Travail Humain*, 51(1) pp. 39--64.

Roth. E. M. and Woods, D. D. (1989). Cognitive Task Analysis: An approach to knowledge acquisition for intelligent system design. In G. Guida and C. Tasso (Eds.), *Topics in Expert System Design*, New York: North-Holland.

Seagull Technology, Inc. (1990). Center-TRACON Automation System Description to Support an Operational Concept Document. Report# 90112-03. November, 1990. Washington, DC: Federal Aviation Administration.

Shafto, M. G. and Remington, R. W. (April, 1990). Building human interfaces to fault diagnostic expert systems II: Interface development for a complex, real-time system. CHI'90 workshop on computer-human interaction in aerospace systems. Seattle, WA.

Smith, P. J., Giffin, W. C., Rockwell, T. H., and Thomas, M. (1986). Modeling fault diagnosis as the activation and use of a frame system. *Human Factors, 28*(6), pp. 703-716.

Van Cott, H. P. and Kincade, R. G., (Eds.) (1972). *Human engineering guide to equipment design*. Washington, D.C.: U.S. Government Printing Office.

Vicente, K. J. and Rasmussen, J. (1990). The ecology of human-machine systems II: Mediating "direct perception" in complex work domains. *Ecological Psychology, 2*, 207-249.

Wickens, C. D. (1992). Process control and automation. (Ch. 12). In *Engineering psychology and human performance*. New York, NY: HarperCollins.

Wiener, E. L. (1989). Human Factors of Advanced Technology ("Glass Cockpit") Transport Aircraft. Technical Report 117528, NASA.

Woods, D. D. (1984). Visual Momentum: A concept to improve the cognitive coupling of person and computer. *International Journal of Man-Machine Studies, 21*, 229--244.

Woods, D. D. (1986a). Cognitive Technologies: The design of joint human-machine cognitive systems. *AI Magazine, 6*, 86--92.

Woods, D. D. (1986b). Paradigms for intelligent decision support. In E. Hollnagel, G. Mancini, and D. Woods (Eds.) *Intelligent Decision Support in Process Environments.* Springer-Verlag.

Woods, D. D. (1988a). Coping with complexity: The psychology of human behavior in complex systems. In L. P. Goodstein, H. B. Andersen, and S. E. Olsen (Eds), *Mental Models, Tasks and Errors,* London: Taylor & Francis.

Woods, D. D. (1988b). The significance messages concept for intelligent adaptive data display. CSEL Report 1988-015. Columbus, OH: The Ohio State University.

Woods, D. D. (1991). The Cognitive Engineering of Problem Representations. In G. R. S. Weir and J. L. Alty (Eds.), *Human-Computer Interaction and Complex Systems,* London: Academic Press.

Woods, D. D. (1992). Cognitive activities and aiding strategies in dynamic fault management. CSEL Report 1992-TR-05. Columbus, OH: The Ohio State University.

Woods, D. D. (in press). Towards a theoretical base for representation design in the computer medium: Ecological perception and aiding human cognition. In Flach, J. M., Hancock, P. A., Caird, J. K., and Vicente, K. J. (Eds.) *An ecological approach to human machine systems I: A global perspective.* Hillsdale, NJ: Erlbaum.

Woods, D. D. and Elias, G. (1988). Significance Messages: An integral display concept. In *Proceedings of the Human Factors Society 32nd Annual Meeting* Santa Monica, CA: The Human Factors Society.

Woods, D. D., Elm, W. C., and Easter, J. R. (1986). The disturbance board concept for intelligent support of fault management tasks. In *Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power,* American Nuclear Society/European Nuclear Society.

Woods, D. D. and Hollnagel, E. (1987). Mapping cognitive demands in complex problem-solving worlds. *International Journal of Man-Machine Studies, 26,* pp. 257-275.

Woods, D. D., Johannesen, L., and Potter, S. S. (October, 1991). Human interaction with intelligent systems: An overview and bibliography. *SIGART Bulletin,* 2(5). New York: ACM. pp. 39-50.

Woods, D. D., Johannesen, L., and Potter, S. S. (1992). The sophistry of guidelines: Revisiting recipes for color use in human-computer interface design. In *Proceedings of the Human Factors Society 36th Annual Meeting.* Santa Monica, CA: The Human Factors Society.

Woods, D. D., O'Brien, J. F., and Hanes, L. F. (1987). Human factors challenges in process control: The case of nuclear power plants. In G. Salvendy (Ed.), *Handbook of human factors.* New York: Wiley. pp. 1724-1770.

Woods, D. D., Potter, S. S., Johannesen, L., and Holloway, M. (1991a). Human Interaction with Intelligent Systems: Volume I – Trends, Problems, New Directions. CSEL Report 1991-001. Columbus, OH: The Ohio State University.

Woods, D. D., Potter, S. S., Johannesen, L., and Holloway, M. (1991b). Human Interaction with Intelligent Systems: Volume II – Case Study Reports. CSEL Report 1991-001. Columbus, OH: The Ohio State University.

Woods, D. D. and Roth, E. M. (1988a). Cognitive Systems Engineering. In M. Helander (Ed.). *Handbook of Human-Computer Interaction.* Elsevier Science Publishers B. V. (North-Holland). pp. 3-43.

Woods, D. D. and Roth, E. M. (1988b). Aiding human performance: II. From cognitive analysis to support systems. *Le Travail Humain, 51*(2) pp. 139-171.

Woods, D. D., Roth, E. M., and Bennett, K. B. (1990). Explorations in joint human-machine cognitive systems. In S. Robertson, W. Zachary, and J. Black (Eds.), *Cognition, Computing and Cooperation,* Norwood, NJ: Ablex Publishing.

Woods, D. D., Wise, J., and Hanes, L. F. (1981). An evaluation of nuclear power plant safety parameter display systems. *In Proceedings of the 24th Annual Meeting of the Human Factors Society.* Santa Monica, CA: The Human Factors Society.